



日本国特許庁  
JAPAN PATENT OFFICE

10/603,486 filed 6-25-03  
Naomi Shiragami et al.

JW Price  
949-253-4920

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日  
Date of Application:

2002年 6月26日

出願番号  
Application Number:

特願2002-186589

[ST.10/C]:

[JP2002-186589]

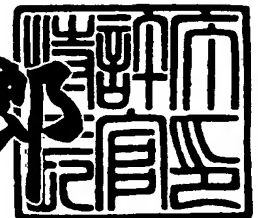
出願人  
Applicant(s):

松下電器産業株式会社

2003年 6月25日

特許庁長官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2003-3050037

【書類名】 特許願

【整理番号】 2969530011

【提出日】 平成14年 6月26日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 株式会社 松下ソ  
                        フトリサーチ内

    【氏名】 白髪 直美

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式  
                        会社内

    【氏名】 羽藤 和美

【特許出願人】

    【識別番号】 000005821

    【氏名又は名称】 松下電器産業株式会社

【代理人】

    【識別番号】 100090446

    【弁理士】

    【氏名又は名称】 中島 司朗

【手数料の表示】

    【予納台帳番号】 014823

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

    【包括委任状番号】 9003742

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ管理システム

【特許請求の範囲】

【請求項 1】 可搬型の記録媒体に格納された暗号化コンテンツを、管理装置から取得した復号鍵を用いて再生装置により再生するコンテンツ管理システムであって、

前記管理装置は、前記暗号化コンテンツを復号する為の復号鍵と前記暗号化コンテンツの開示の可否を示す開示情報とを対応付けて保持しており、

前記記録媒体は、暗号鍵を用いて暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求する鍵要求プログラムとを格納しており、

前記再生装置は、前記記録媒体から前記鍵要求プログラムを読み出して実行し

、  
前記管理装置は、前記再生装置からの要求を受けると、前記暗号化コンテンツの開示の可否を前記開示情報に応じて判断し、開示可と判断した場合に前記復号鍵を前記再生装置へ送信し、

前記再生装置は、前記管理装置から前記復号鍵を受信し、前記記録媒体から前記暗号化コンテンツを読み出して前記復号鍵を用いて復号し再生する

ことを特徴とするコンテンツ管理システム。

【請求項 2】 前記再生装置は、

前記記録媒体から前記鍵要求プログラムを読み出して解読し実行する鍵要求プログラム実行手段と、

前記管理装置から前記復号鍵を受信する復号鍵受信手段と、

前記記録媒体から前記暗号化コンテンツを読み出すコンテンツ読出手段と、

前記復号鍵を用いて前記暗号化コンテンツを復号し再生する再生手段とを備え

、  
前記管理装置は、

前記暗号化コンテンツを復号する為の復号鍵を記憶している鍵記憶手段と、

前記暗号化コンテンツの開示の可否を示す開示情報を記憶している開示情報記憶手段と、

前記再生装置からの要求を受けて、前記開示情報に応じて前記暗号化コンテンツの開示の可否を判断する開示判断手段と、

開示可と判断した場合に、前記復号鍵を前記再生装置へ送信する復号鍵送信手段と

を備えることを特徴とする請求項 1 に記載のコンテンツ管理システム。

【請求項 3】 管理装置から取得する復号鍵を用いて再生装置により再生される暗号化コンテンツを格納した可搬型の記録媒体であって、

前記管理装置は、前記暗号化コンテンツの復号鍵を保持しており、

前記記録媒体は、暗号鍵により暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求するための鍵要求プログラムとを格納している

ことを特徴としている記録媒体。

【請求項 4】 可搬型の記録媒体に格納された暗号化コンテンツを復号する為の復号鍵を保持し、前記復号鍵を再生装置に送信する管理装置であって、

前記記録媒体は、暗号鍵を用いて暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求する鍵要求プログラムとを格納しており、

前記管理装置は、

前記暗号化コンテンツを復号する為の復号鍵を記憶している鍵記憶手段と、

前記暗号化コンテンツの開示の可否を示す開示情報を記憶している開示情報記憶手段と、

前記再生装置からの要求を受けて、前記開示情報に応じて前記暗号化コンテンツの開示の可否を判断する開示判断手段と、

開示可と判断した場合に、前記復号鍵を前記再生装置へ送信する復号鍵送信手段と

を備えることを特徴とする管理装置。

【請求項 5】 前記開示情報記憶手段は、前記記録媒体及び前記再生装置を有する利用者を識別する利用者識別子を含み、前記利用者識別子により識別される利用者に対する前記暗号化コンテンツの開示の可否を示す開示情報を記憶しており、

前記開示判断手段は、前記再生装置から前記利用者識別子を含む要求を受け付

けると、前記開示情報を用いて、前記利用者識別子により識別される利用者に対する前記暗号化コンテンツの開示の可否を判断する

ことを特徴とする請求項 4 に記載の管理装置。

【請求項 6】 前記記録媒体は、それぞれ異なる暗号鍵で暗号化された複数個の暗号化コンテンツとそれぞれの暗号化コンテンツを一意に識別するコンテンツ識別子とを対応付けて格納しており、

前記開示情報記憶手段は、複数の暗号化コンテンツについて、暗号化コンテンツ毎に前記開示情報を記憶しており、

前記開示判断手段は、前記利用者識別子と利用を所望する暗号化コンテンツを識別するコンテンツ識別子とを含む要求を受け付けると、前記開示情報を用いて、前記利用者識別子により識別される利用者に対する前記コンテンツ識別子により識別される暗号化コンテンツの開示の可否を判断する

ことを特徴とする請求項 5 に記載の管理装置。

【請求項 7】 前記開示情報は、暗号化コンテンツの開示が許可されている期間を示す開示期間、機密を示す機密区分、内容を示す分野の内の少なくとも一つを含むコンテンツ開示情報と、利用者の利用可能期間、利用可能機密区分、利用可能分野の内の少なくとも一つを含む利用者情報とを含み、

前記開示判断手段は、前記コンテンツ情報と前記利用者情報とを参照することにより、前記利用者に対する前記暗号化コンテンツの開示の可否を判断する

ことを特徴とする請求項 6 に記載の管理装置。

【請求項 8】 前記管理装置は、更に、

前記開示情報を更新する為に用いる更新情報の入力を受け付ける更新受付手段と、

受け付けた更新情報に応じて、前記開示情報を更新する更新手段とを備える

ことを特徴とする請求項 4 に記載の管理装置。

【請求項 9】 前記管理装置は、更に、

前記再生装置からの要求を受け付けると、前記記録媒体及び前記再生装置を有する利用者を一意に識別する利用者識別子と前記暗号化コンテンツを一意に識別するコンテンツ識別子とを含む履歴情報を生成する履歴情報生成手段と、

生成した履歴情報を蓄積して記憶する履歴情報記憶手段とを備える  
ことを特徴とする請求項 4 に記載の管理装置。

【請求項 1 0】 可搬型の記録媒体に格納された暗号化コンテンツを、管理装置から取得した復号鍵を用いて再生する再生装置であって、

前記管理装置は、前記暗号化コンテンツの復号鍵を保持しており、

前記記録媒体は、暗号鍵により暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求するための鍵要求プログラムとを格納しており、

前記再生装置は、

前記記録媒体から、前記鍵要求プログラムを読み出して実行し、前記管理装置から前記復号鍵を受信すると、前記記録媒体から前記暗号化コンテンツを読み出して復号し再生する

ことを特徴とする再生装置。

【請求項 1 1】 前記コンテンツ管理システムは、更に、当該システムの管理者が有する管理者装置を備え、

前記管理者装置は、前記開示情報を更新する為に用いる更新情報の入力を受け付け、受け付けた更新情報を前記管理装置へ送信し、

前記管理装置は、前記管理者装置から前記更新情報を受信し、受信した更新情報に応じて、前記開示情報を更新する

ことを特徴とする請求項 1 に記載のコンテンツ管理システム。

【請求項 1 2】 前記コンテンツ管理システムは、更に、当該システムの管理者が有する管理者装置を備え、

前記管理装置は、前記再生装置からの要求を受け付けると、前記再生装置を有する利用者を一意に識別する利用者識別子と前記暗号化コンテンツを一意に識別するコンテンツ識別子とを含む履歴情報を生成し、生成した履歴情報を蓄積して記憶し、

前記管理者装置は、前記管理装置に対して前記履歴情報の送信を要求する履歴要求の入力を受け付け、受け付けた履歴要求を前記管理装置へ送信し、

前記管理装置は、前記管理者装置から前記履歴要求を受信し、記憶している前記履歴情報を読み出して前記管理者装置へ送信する

ことを特徴とする請求項 1 に記載のコンテンツ管理システム。

【請求項 1 3】 暗号鍵を用いて暗号化された暗号化コンテンツを復号する為の復号鍵と前記暗号化コンテンツの開示の可否を示す開示情報とを対応付けて保持している管理装置と、前記暗号化コンテンツと前記管理装置に対して前記復号鍵を要求する鍵要求プログラムとを格納している可搬型の記録媒体とを備えるコンテンツ管理システムで用いられるコンテンツ管理方法であって、

前記記録媒体から前記鍵要求プログラムを読み出して実行するプログラム実行ステップと、

再生装置からの要求を受けると、前記暗号化コンテンツの開示の可否を前記開示情報に応じて判断し、開示可と判断した場合に前記復号鍵を前記再生装置へ送信する復号鍵送信ステップと、

前記管理装置から前記復号鍵を受信し、前記記録媒体から前記暗号化コンテンツを読み出して前記復号鍵を用いて復号し再生する再生ステップと

を含むことを特徴とするコンテンツ管理方法。

【請求項 1 4】 暗号鍵を用いて暗号化された暗号化コンテンツを復号する為の復号鍵と前記暗号化コンテンツの開示の可否を示す開示情報とを対応付けて保持している管理装置と、前記暗号化コンテンツと前記管理装置に対して前記復号鍵を要求する鍵要求プログラムとを格納している可搬型の記録媒体とを備えるコンテンツ管理システムで用いられるコンテンツ管理プログラムであって、

前記記録媒体から前記鍵要求プログラムを読み出して実行するプログラム実行ステップと、

再生装置からの要求を受けると、前記暗号化コンテンツの開示の可否を前記開示情報に応じて判断し、開示可と判断した場合に前記復号鍵を前記再生装置へ送信する復号鍵送信ステップと、

前記管理装置から前記復号鍵を受信し、前記記録媒体から前記暗号化コンテンツを読み出して前記復号鍵を用いて復号し再生する再生ステップと

を含むことを特徴とするコンテンツ管理プログラム。

【請求項 1 5】 暗号鍵を用いて暗号化された暗号化コンテンツを復号する為の復号鍵と前記暗号化コンテンツの開示の可否を示す開示情報とを対応付けて保

持している管理装置と、前記暗号化コンテンツと前記管理装置に対して前記復号鍵を要求する鍵要求プログラムとを格納している可搬型の記録媒体とを備えるコンテンツ管理システムで用いられるコンテンツ管理プログラムを記録しているコンピュータ読み取り可能な記録媒体であって、

前記コンテンツ管理プログラムは、

前記記録媒体から前記鍵要求プログラムを読み出して実行するプログラム実行ステップと、

再生装置からの要求を受けると、前記暗号化コンテンツの開示の可否を前記開示情報に応じて判断し、開示可と判断した場合に前記復号鍵を前記再生装置へ送信する復号鍵送信ステップと、

前記管理装置から前記復号鍵を受信し、前記記録媒体から前記暗号化コンテンツを読み出して前記復号鍵を用いて復号し再生する再生ステップと

を含むことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、可搬型の記録媒体に格納されて利用者に配布されたコンテンツを管理する技術に関する。

【0002】

【従来の技術】

コンテンツを利用者に配信する方法の一つに、コンテンツを記録媒体に格納して利用者に配布する方法がある。記録媒体に格納され利用者に配信されたコンテンツは、際限なく再生又はコピーされる可能性があるため、コンテンツの不正利用を防止することが必要である。

【0003】

そこで、コンテンツを暗号化した暗号化コンテンツと暗号化コンテンツを復号する為の復号鍵と共に、コンテンツの再生可能回数などを示す権利情報を記録媒体に格納し、当該権利情報に従い、当該復号鍵を用いてコンテンツを復号することが行われている。



## 【 0 0 0 4 】

## 【発明が解決しようとする課題】

上記の様に、暗号化した暗号化コンテンツと共に権利情報を記録媒体に格納して利用者に配布すると、権利情報により暗号化コンテンツの復号を制限することが可能である。しかしながら、システムの管理者が権利情報を更新するために、既に配布されている記録媒体を回収するのは極めて困難であり、管理者の手元を離れ利用者に配布された記録媒体に格納されている権利情報を操作することはできないという問題がある。

## 【 0 0 0 5 】

本発明は、上記問題点に鑑み、記録媒体に格納された暗号化コンテンツの復号に制限を課しつつ、管理者により権利情報を操作することが可能なコンテンツ管理システムを提供することを目的とする。

## 【 0 0 0 6 】

## 【課題を解決するための手段】

上記目的を達成するために、本発明は、可搬型の記録媒体に格納された暗号化コンテンツを、管理装置から取得した復号鍵を用いて再生装置により再生するコンテンツ管理システムであって、前記管理装置は、前記暗号化コンテンツを復号する為の復号鍵と前記暗号化コンテンツの開示の可否を示す開示情報とを対応付けて保持し、前記記録媒体は、暗号鍵を用いて暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求する鍵要求プログラムとを格納しており、前記再生装置は、前記記録媒体から前記鍵要求プログラムを読み出して実行し、前記管理装置は、前記再生装置からの要求を受けると、前記暗号化コンテンツの開示の可否を前記開示情報に応じて判断し、開示可と判断した場合に前記復号鍵を前記再生装置へ送信し、前記再生装置は、前記管理装置から前記復号鍵を受信し、前記記録媒体から前記暗号化コンテンツを読み出して前記復号鍵を用いて復号し再生することを特徴とする。

## 【 0 0 0 7 】

さらに、本発明は、管理装置から取得する復号鍵を用いて再生装置により再生される暗号化コンテンツを格納した可搬型の記録媒体であって、前記管理装置は

、前記暗号化コンテンツの復号鍵を保持し、前記記録媒体は、暗号鍵により暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求するための鍵要求プログラムとを格納していることを特徴とする。

## 【 0 0 0 8 】

さらに、本発明は、可搬型の記録媒体に格納された暗号化コンテンツを復号する為の復号鍵を保持し、前記復号鍵を再生装置に送信する管理装置であって、前記記録媒体は、暗号鍵を用いて暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求する鍵要求プログラムとを格納しており、前記管理装置は、前記暗号化コンテンツを復号する為の復号鍵と前記暗号化コンテンツの開示の可否を示す開示情報とを記憶しており、前記再生装置からの要求を受けて、前記開示情報に応じて前記暗号化コンテンツの開示の可否を判断し、開示可と判断した場合に、前記復号鍵を前記再生装置へ送信することを特徴とする。

## 【 0 0 0 9 】

さらに、本発明は、可搬型の記録媒体に格納された暗号化コンテンツを、管理装置から取得した復号鍵を用いて再生する再生装置であって、前記管理装置は、前記暗号化コンテンツの復号鍵を保持しており、前記記録媒体は、暗号鍵により暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求するための鍵要求プログラムとを格納しており、前記再生装置は、前記記録媒体から、前記鍵要求プログラムを読み出して実行し、前記管理装置から前記復号鍵を受信すると、前記記録媒体から前記暗号化コンテンツを読み出して復号し再生することを特徴とする。

## 【 0 0 1 0 】

さらに、本発明のコンテンツ管理システムは、当該システムの管理者が有する管理者装置を備え、前記管理者装置は、前記開示情報を更新する為に用いる更新情報の入力を受け付け、受け付けた更新情報を前記管理装置へ送信し、前記管理装置は、前記管理者装置から前記更新情報を受信し、受信した更新情報に応じて、前記開示情報を更新することを特徴とする。

## 【 0 0 1 1 】

さらに、本発明のコンテンツ管理システムは、当該システムの管理者が有する

管理者装置を備え、前記管理装置は、前記再生装置からの要求を受け付けると、前記再生装置を有する利用者を一意に識別する利用者識別子と前記暗号化コンテンツを一意に識別するコンテンツ識別子とを含む履歴情報を生成し、生成した履歴情報を蓄積して記憶し、前記管理者装置は、前記管理装置に対して前記履歴情報の送信を要求する履歴要求の入力を受け付け、受け付けた履歴要求を前記管理装置へ送信し、前記管理装置は、前記管理者装置から前記履歴要求を受信すると、記憶している前記履歴情報を読み出して前記管理者装置へ送信することを特徴とする。

## 【 0 0 1 2 】

## 【発明の実施の形態】

本発明に掛かる実施の形態として、コンテンツ管理システム 1 について図面を参照して説明する。コンテンツとは技術資料を P D F (Portable Document Format) ファイル形式に変換したものである。ここでは 1 個のファイルを 1 個のコンテンツと呼ぶ。コンテンツ管理システム 1 は、企業内において、コンテンツの開示を管理するシステムである。

## 【 0 0 1 3 】

## ＜構成＞

ここでは、コンテンツ管理システム 1 の構成について説明する。

図 1 は、コンテンツ管理システム 1 の構成を示す図である。同図に示す様に、コンテンツ管理システム 1 は、コンテンツ管理サーバ 1 0、ユーザ用クライアント 3 0、提供者用クライアント 5 0 及び管理者用クライアント 4 0 が、イントラネット 6 0 を介して接続されて構成される。また、コンテンツ管理サーバ 1 0 によってコンテンツが格納された記録媒体 2 0 は、予め、管理者から利用者へ配布されている。

## 【 0 0 1 4 】

コンテンツ管理サーバ 1 0 は、当該システムの管理者が有する装置であって、コンテンツの管理に必要な情報をデータベースに格納している。ユーザ用クライアント 3 0 は、当該システムの利用者が有する装置である。管理者用クライアント 4 0 は、当該システムの管理者が有する装置である。提供者用クライアント 5

0 は、当該システムにおけるコンテンツの提供者が有する装置である。

【 0 0 1 5 】

1. コンテンツ管理サーバ 1 0

コンテンツ管理サーバ 1 0 は、コンテンツを暗号化して暗号化コンテンツを生成し、生成した暗号化コンテンツを記録媒体 2 0 に格納する。また、コンテンツ管理サーバ 1 0 は、利用者に配布された記録媒体 2 0 に格納されている暗号化コンテンツの管理に必要な情報をデータベースに格納している。

【 0 0 1 6 】

ここでは、コンテンツ管理サーバ 1 0 の構成について説明する。

図 2 は、コンテンツ管理サーバ 1 0 の構成を示すブロック図である。同図に示す様に、コンテンツ管理サーバ 1 0 は、ゲートウェイ 1 0 1、データベース部 1 0 2、ユーザ認証部 1 0 3、履歴管理部 1 0 4、データベース管理部 1 0 5、コンテンツ記憶部 1 0 6、プログラム記憶部 1 0 7、暗号化部 1 0 8 及び入出力部 1 0 9 から構成される。

【 0 0 1 7 】

コンテンツ管理サーバ 1 0 は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード及びマウスなどから構成されるコンピュータシステムである。前記 RAM 又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することによりコンテンツ管理サーバ 1 0 はその機能を達成する

(1) ゲートウェイ 1 0 1

ゲートウェイ 1 0 1 は、イントラネット 6 0 を介してユーザ認証部 1 0 3 とユーザ用クライアント 3 0 との間で情報の送受信を行う。ゲートウェイ 1 0 1 は、ユーザ認証部 1 0 3 から復号鍵を受け取ると、受け取った復号鍵に base 6 4 変換を施し、イントラネット 6 0 を介してユーザ用クライアント 3 0 へ送信する。また、ゲートウェイ 1 0 1 は、履歴管理部 1 0 4 と提供者用クライアント 5 0 との間で情報の送受信を行う。更に、ゲートウェイ 1 0 1 は、履歴管理部 1 0 4 と管理者用クライアント 4 0、及びデータベース管理部 1 0 5 と管理者用クライ

アント40の間で情報の送受信を行う。

【0018】

(2) データベース部102

データベース部102は、具体的にはハードディスクユニットから構成され、コンテンツの管理に必要な情報である、ユーザ認証テーブル110、ユーザテーブル120、コンテンツテーブル130、復号鍵テーブル140及び履歴テーブル150を格納している。以下、それぞれについて説明する。

【0019】

(ユーザ認証テーブル110)

図3は、ユーザ認証テーブル110のデータ構造を示す図である。ユーザ認証テーブル110は、当該システムを利用する利用者の数と同数のユーザ認証情報から構成される。各ユーザ認証情報は、各利用者と1対1に対応している。ユーザ認証情報の一例であるユーザ認証情報1100は、ユーザID1101、パスワード1102、登録ユーザ1103、登録日1104、更新ユーザ1105及び更新日1106から構成される。

【0020】

ここで、ユーザID1101は、ユーザ認証情報1100に対応する利用者を一意に識別する記号であり、パスワード1102は、ユーザ認証情報1100に対応する利用者が当該システムを利用する際に本人であるかどうかを認証するために用いられる。登録ユーザ1103は、ユーザ認証情報1100をデータベース部102に登録した人物をユーザIDを用いて示したもので、登録日1104は、登録ユーザ1103により識別される人物がユーザ認証情報1100をデータベース部102に登録した日時を示す。更新ユーザ1105は、ユーザID1101及びパスワード1102が上書きされた場合に、上書きした人物をユーザIDを用いて示したもので、更新日1106は、更新ユーザ1105により識別される人物がユーザID1101及びパスワード1102を上書きした日時を示す。なお、ユーザ認証情報1100がデータベース部102に登録された後、ユーザID1101及びパスワード1102の上書きがされない場合は、更新ユーザ1105及び更新日1106は何も記述されない。

## 【 0 0 2 1 】

## (ユーザテーブル 1 2 0)

図 4 は、ユーザテーブル 1 2 0 のデータ構造を示す図である。ユーザテーブル 1 2 0 は、当該システムを利用する利用者の数と同数のユーザ情報を含み、各ユーザ情報は、各利用者と 1 対 1 に対応している。ユーザ情報の一例であるユーザ情報 1 2 0 0 は、ユーザ ID 1 2 0 1、利用可能期間（開始） 1 2 0 2、利用可能期間（終了） 1 2 0 3、利用可能件数 1 2 0 4、利用可能分野コード 1 2 0 5、利用可能公開区分 1 2 0 6、登録ユーザ 1 2 0 7、登録日 1 2 0 8、更新ユーザ 1 2 0 9、及び更新日 1 2 1 0 から構成される。

## 【 0 0 2 2 】

ここで、ユーザ ID 1 2 0 1 は、ユーザ情報 1 2 0 0 に対応する利用者を一意に識別する為の記号である。利用可能期間（開始） 1 2 0 2 は、コンテンツ利用の権利が当該利用者に与えられた日時を示し、利用可能期間（終了） 1 2 0 3 は、当該利用者のコンテンツ利用の権利が消失する日時を示す。利用可能件数 1 2 0 4 は、当該利用者が利用可能であるコンテンツの数である。利用可能分野コード 1 2 0 5 は、当該利用者が利用可能であるコンテンツの分野を示す記号である。利用可能公開区分 1 2 0 6 は、当該利用者が利用可能であるコンテンツの公開区分を示す。利用可能公開区分 1 2 0 6 は、「無」、「秘」、「厳秘」、「極秘」の 4 種類の何れかであり、コンテンツの公開区分も「無」、「秘」、「厳秘」、「極秘」の 4 種類の何れかである。利用可能公開区分 1 2 0 6 が「無」である場合、当該ユーザは、公開区分が「無」のコンテンツのみを利用することが出来る。利用可能公開区分 1 2 0 6 が「秘」である場合、当該ユーザは、公開区分が「秘」及び「無」のコンテンツを利用することが出来る。利用可能公開区分 1 2 0 6 が「厳秘」である場合、当該ユーザは、公開区分が「厳秘」、「秘」及び「無」のコンテンツを利用することが出来る。利用可能公開区分 1 2 0 6 が「極秘」である場合、当該ユーザは、公開区分が「極秘」、「厳秘」、「秘」及び「無」のコンテンツを利用することが出来る。また、登録ユーザ 1 2 0 7、登録日 1 2 0 8、更新ユーザ 1 2 0 9 及び更新日 1 2 1 0 については、上述したユーザ認証情報 1 1 0 0 に含まれるものと同様であるため説明を省略する。

## 【0023】

## (コンテンツテーブル130)

図5は、コンテンツテーブル130のデータ構造を示す図である。コンテンツテーブル130は、記録媒体20に格納されて利用者に配送されているコンテンツの数と同数のコンテンツ情報を含み、各コンテンツ情報は、各コンテンツと1対1に対応している。コンテンツ情報の一例であるコンテンツ情報1300は、コンテンツID1301、公開期間(開始)1302、公開期間(終了)1303、分野コード1304、公開区分1305、登録ユーザ1306、登録日1307、更新ユーザ1308、更新日1309及び作成者IDから構成される。

## 【0024】

ここで、コンテンツID1301は、コンテンツ情報1300に対応するコンテンツを一意に識別する記号である。公開期間(開始)1302は、当該コンテンツが利用者に対して公開される日時であり、公開期間(終了)1303は、利用者に対して公開されている当該コンテンツの開示が終了する日時である。分野コード1304は、当該コンテンツの分野を示す記号である。コンテンツ管理システム1で扱うコンテンツは全てその内容に応じて、「暗号」、「画像処理」、「デジタル放送」などにグループ分けされており、これらを分野と呼ぶ。分野コードは、これら分野を一意に識別するために記号で表したものである。公開区分1305は、当該コンテンツの機密に係る公開制限の程度を表したものであり、「無」、「秘」、「厳秘」、「極秘」の4種類の何れかである。なお、登録ユーザ1306、登録日1307、更新ユーザ1308及び更新日1309については、上述したユーザ認証情報1100に含まれるものと同様であるため説明を省略する。作成者IDは、コンテンツ情報1300に対応するコンテンツである技術資料を作成した提供者を一意に識別する記号である。

## 【0025】

## (復号鍵テーブル140)

図6は、復号鍵テーブル140のデータ構造を示す図である。復号鍵テーブル140は、記録媒体20に格納されて利用者に配送されているコンテンツの数と

同数の復号鍵情報を含み、各復号鍵情報は、各コンテンツと1対1に対応している。復号鍵情報の一例である復号鍵情報1400は、コンテンツID1401、復号鍵1402、登録ユーザ1403、登録日1404、更新ユーザ1405及び更新日1406から構成される。

#### 【0026】

コンテンツID1401は、復号鍵情報1400に対応するコンテンツを一意に識別する記号である。復号鍵1402は、当該コンテンツを復号する際に用いられる復号鍵である。登録ユーザ1403、登録日1404、更新ユーザ1405及び更新日1406については、上述したユーザ認証情報1100に含まれるものと同様であるため説明を省略する。

#### 【0027】

##### (履歴テーブル150)

図7は、履歴テーブル150のデータ構造を示す図である。履歴テーブル150は、利用者がコンテンツを利用した回数と同数の履歴情報を含み。履歴情報の一例である履歴情報1500は、ユーザID1507、コンテンツID1502及び利用日1503から構成される。

#### 【0028】

ここで、ユーザID1501は、履歴情報1500に対応するコンテンツを利用した利用者を一意に識別する記号であり、コンテンツID1502は、当該コンテンツを一意に識別する記号である。利用日1503は、ユーザIDにより識別される利用者が、当該コンテンツを利用した日時を示す。

##### (3) ユーザ認証部103

ユーザ認証部103は、マイクロプロセッサ及びRAM等から構成される。ユーザ認証部103は、ゲートウェイ101及びイントラネット60を介してユーザ用クライアント30からユーザID及びパスワードを受信する。ユーザ認証部103は、データベース部102のユーザ認証テーブル110から、受信した前記ユーザIDを含むユーザ認証情報を読み出し、受信した前記パスワードが読み出したユーザ認証情報に含まれるパスワードと一致するか否かを判断することによりユーザ認証を行う。



## 【 0 0 2 9 】

ユーザ認証部 1 0 3 は、パスワードの不一致により認証に失敗した場合、パスワード間違えを示すエラーメッセージを表示する為の指示をユーザ用クライアント 3 0 へ送信する。また、受信した前記ユーザ I D を含むユーザ認証情報が無い場合にも、未登録を示すエラーメッセージを表示する為の指示をユーザ用クライアント 3 0 へ送信する。

## 【 0 0 3 0 】

ユーザ認証部 1 0 3 は、パスワードの一致により認証に成功した場合、更に、データベース部 1 0 2 のユーザテーブル 1 2 0 から受信した前記ユーザ I D と同じユーザ I D を含むユーザ情報を読み出す。ユーザ認証部 1 0 3 は、読み出したユーザ情報に含まれる利用可能期間（開始）及び利用可能期間（終了）を参照して、現在が当該利用者の利用可能期間であるか否か判断する。現在が利用可能期間である場合、ユーザ認証部 1 0 3 は、認証に成功したことを示す指示をユーザ用クライアント 3 0 に送信する。現在が当該利用者の利用可能期間でない場合、ユーザ認証部 1 0 3 は、利用可能期間外であることを示すエラーメッセージをユーザ用クライアント 3 0 に送信する。

## 【 0 0 3 1 】

ユーザ認証部 1 0 3 は、ゲートウェイ 1 0 1 及びイントラネット 6 0 を介してユーザ用クライアント 3 0 から、ユーザ I D とコンテンツ I D とを受信する。ユーザ認証部 1 0 3 は、受信した前記ユーザ I D に対応する利用者に対して、受信した前記コンテンツ I D に対応するコンテンツの復号鍵を送信するか否かを判断する。復号鍵を送信すると判断した場合、ユーザ認証部 1 0 3 は、データベース部 1 0 2 から読み出した復号鍵情報に含まれる復号鍵をゲートウェイ 1 0 1 へ出力する。復号鍵を送信しないと判断した場合、ユーザ認証部 1 0 3 は、エラーメッセージをユーザ用クライアント 3 0 へ送信する。復号鍵を送信するか否かの判断についての詳細は後述する。

## 【 0 0 3 2 】

## ( 4 ) 履歴管理部 1 0 4

履歴管理部 1 0 4 は、マイクロプロセッサ及び R A M などから構成される。履

履歴管理部 1 0 4 は、管理者用クライアント 4 0 及び提供者用クライアント 5 0 に  
対して利用者が復号鍵を要求したコンテンツに関する情報を提供する。

具体的には、履歴管理部 1 0 4 は、管理者用クライアント 4 0 から要求を受け  
付けると、データベース部 1 0 2 の履歴テーブル 1 5 0 から履歴情報を読み出し  
、読み出した履歴情報をゲートウェイ 1 0 1 及びイントラネット 6 0 を介して管  
理者用クライアント 4 0 へ送信する。

【 0 0 3 3 】

また、履歴管理部 1 0 4 は、提供者用クライアント 5 0 から要求を受け付け  
ると、データベース部に格納されているコンテンツ情報及び履歴情報に基づき、当  
該提供者が作成したコンテンツに関する履歴情報を読み出し、読み出した履歴情  
報をゲートウェイ 1 0 1 及びイントラネット 6 0 を介して提供者用クライアント  
5 0 へ送信する。

【 0 0 3 4 】

(5) データベース管理部 1 0 5

データベース管理部 1 0 5 は、マイクロプロセッサ及び R A M などから構成さ  
れる。データベース管理部 1 0 5 は、管理者用クライアント 4 0 からの要求を受  
け付け、データベース部 1 0 2 に格納されているデータを読み出し、読み出した  
データを前記要求に従い更新する。

【 0 0 3 5 】

例として、データベース管理部 1 0 5 は、データベース部 1 0 2 のユーザ情報  
1 2 0 に含まれるユーザ情報の利用可能期間（終了）を変更することにより、当  
該利用者の利用可能期間を延長、又は短縮する。また、データベース管理部 1 0  
5 は、データベース部 1 0 2 のコンテンツテーブル 1 3 0 に含まれるコンテン  
ツの公開期間（終了）を変更することにより、当該コンテンツの開示期間を延長、  
又は短縮する。また、コンテンツ情報の公開区分を「厳秘」から「秘」に変更す  
ることにより、当該コンテンツの機密に係る公開制限を緩和したり、「秘」から  
「無」に変更することにより、公開制限を解除したりする。

【 0 0 3 6 】

以上の様に、データベース管理部 1 0 5 は、管理者用クライアント 4 0 からの

要求に従い、データベース部 1 0 2 に格納されている、ユーザ認証情報、ユーザ情報、コンテンツ情報及び復号鍵情報に含まれる各データを更新する。

(6) コンテンツ記憶部 1 0 6

コンテンツ記憶部 1 0 6 は、ハードディスクユニットから構成され、複数のコンテンツをそれぞれコンテンツ ID と対応付けて格納している。コンテンツ記憶部 1 0 6 が記憶しているコンテンツは、暗号化部 1 0 8 により暗号化されて、記録媒体 2 0 に格納される。

【 0 0 3 7 】

(7) プログラム記憶部 1 0 7

プログラム記憶部 1 0 7 は、暗号化部 1 0 8 が生成する暗号化コンテンツと共に記録媒体 2 0 に格納されるコンピュータプログラム及びデータを記憶している。コンピュータプログラム及びデータの詳細は後述する。プログラム記憶部 1 0 7 は、入出力部 1 0 9 からの要求に応じて前記コンピュータプログラム及びデータを入出力部 1 0 9 へ出力する。

【 0 0 3 8 】

(8) 暗号化部 1 0 8

暗号化部 1 0 8 は、コンテンツ記憶部 1 0 6 に格納されているコンテンツ ID と当該コンテンツ ID に対応するコンテンツとを読み出し、読み出したコンテンツ ID と同じコンテンツ ID を含む復号鍵情報を、データベース部 1 0 2 の復号鍵テーブル 1 4 0 から読み出す。暗号化部 1 0 8 は、読み出した復号鍵を用いてコンテンツに暗号アルゴリズム  $E_1$  を施して暗号化コンテンツを生成する。ここで、前記暗号アルゴリズム  $E_1$  の一例は DES (Data Encryption Standard) である。暗号化部 1 0 8 は、コンテンツ記憶部 1 0 6 に格納されている全てのコンテンツについて、前述の処理を行う。暗号化部 1 0 8 は、生成した全ての暗号化コンテンツを、入出力部 1 0 9 に出力する。

【 0 0 3 9 】

(9) 入出力部 1 0 9

入出力部 1 0 9 は、具体的には CD レコーダユニットであり、記録媒体 2 0 が装着されると以下の様に、記録媒体 2 0 に情報を書き込む。

入出力部 1 0 9 は、暗号化部 1 0 8 から複数個の暗号化コンテンツを受け取る。入出力部 1 0 9 は、全ての暗号化コンテンツを受け取ると、プログラム記憶部 1 0 7 へコンピュータプログラム及びデータの出力を要求する。入出力部 1 0 9 は、プログラム記憶部 1 0 7 からコンピュータプログラム及びデータを受け取り、暗号化コンテンツとコンピュータプログラムとデータとを記録媒体 2 0 に書き込む。

#### 【 0 0 4 0 】

##### 2. 記録媒体 2 0

記録媒体 2 0 は、コンテンツ管理サーバ 1 0 により暗号化コンテンツとコンピュータプログラムとが格納されて、利用者へ配布されている。

図 8 に示す様に、記録媒体 2 0 は、暗号化コンテンツ 2 0 1、暗号化コンテンツインデックス 2 0 2、インデックス復号鍵情報 2 0 3、画面制御情報 2 0 4、復号鍵要求プログラム 2 0 5 及びコンテンツインデックス出力プログラム 2 0 6 を格納している。記録媒体 2 0 は、具体的には C D - R O M であって、ユーザ用クライアント 3 0 の入出力部 3 0 6 に装着して用いる。

#### 【 0 0 4 1 】

暗号化コンテンツ 2 0 1 は、ここではコンテンツ管理サーバ 1 0 により記録媒体 2 0 に格納された全ての暗号化コンテンツを表す。

暗号化コンテンツインデックス 2 0 2 は、記録媒体 2 0 に格納されている全ての暗号化コンテンツについて、コンテンツ毎に分野、コンテンツ I D、作成者及び文書インデックスを記述したものである。ここで文書インデックスはコンテンツのタイトルである。なお、暗号化コンテンツインデックス 2 0 2 は、予め、暗号アルゴリズム  $E_2$  を施され、暗号化されている。ここで、前記暗号アルゴリズム  $E_2$  の一例は D E S (Data Encryption Standard) である。

#### 【 0 0 4 2 】

インデックス復号鍵情報 2 0 3 は、暗号化コンテンツインデックス 2 0 2 を復号するために用いる復号鍵である。

画面制御情報 2 0 4 は、ユーザ認証画面制御情報、コンテンツインデックス画面制御情報、コンテンツ検索画面制御情報、検索結果画面制御情報、復号確認画

面制御情報及び復号結果画面制御情報を含む。各画面制御情報は、ユーザ認証画面 3 1 0、コンテンツインデックス画面 3 2 0、コンテンツ検索画面 4 1 0、検索結果画面 5 1 0、復号確認画面 6 1 0 及び復号結果画面 7 1 0 を生成するために用いられる。各画面についての詳細は後述する。

#### 【 0 0 4 3 】

復号鍵要求プログラム 2 0 5 及びコンテンツインデックス出力プログラム 2 0 6 は、記録媒体 2 0 がユーザ用クライアント 3 0 の入出力部 3 0 6 に装着された状態において、ユーザ用クライアント 3 0 の入力部 3 0 2 がユーザの操作により復号鍵要求プログラム 2 0 5 及びコンテンツインデックス出力プログラム 2 0 6 の実行指示を受け付けた場合に、ユーザ用クライアント 3 0 の入出力部 3 0 6 が復号鍵要求プログラム 2 0 5 及びコンテンツインデックス出力プログラム 2 0 6 を読み込み、ユーザ用クライアント 3 0 の制御部 3 0 4 により実行される。

#### 【 0 0 4 4 】

##### ＜復号鍵要求プログラム 2 0 5 の動作＞

図 9 は、復号鍵要求プログラム 2 0 5 の動作を示すフローチャートである。

ユーザ認証画面を出力し、ユーザの入力によりユーザ ID とパスワードとを受け付ける（ステップ S 2 0 1）。受け付けたユーザ ID とパスワードとをコンテンツ管理サーバ 1 0 へ送信する。認証に失敗したことを示す情報をコンテンツ管理サーバ 1 0 から受信すると（ステップ S 2 0 2 で N O）、エラーメッセージを出力する（ステップ S 2 0 4）。認証成功したことを示す情報をコンテンツ管理サーバ 1 0 から受信すると（ステップ S 2 0 2 で Y E S）、コンテンツインデックスを出力する（ステップ S 2 0 3）。

#### 【 0 0 4 5 】

続いて、ユーザの入力を受け付け（ステップ S 2 0 5）、コンテンツの選択を受け付けたか否か判断する。コンテンツの選択を受け付けた場合（ステップ S 2 0 6 で Y E S）、コンテンツ管理サーバ 1 0 に対して復号鍵を要求し（ステップ S 2 0 8）、処理を終了する。

コンテンツの選択を受け付けない場合（ステップ S 2 0 6 で N O）、検索の要求を受け付けたか否か判断する。検索の要求を受け付けない場合（ステップ S 2

07でNO)、終了の要求を受け付けたか否か判断する。終了の要求を受け付けた場合(ステップS209でYES)、処理を終了する。

#### 【0046】

終了の要求を受け付けない場合(ステップS209でNO)、ステップS205に戻り処理を続ける。検索の要求を受け付けた場合(ステップS207でYES)、コンテンツ検索画面を出力し(ステップS210)、ユーザの入力を受け付ける(ステップS211)。受け付けた入力情報に基づきコンテンツを検索する(ステップS212)。検索結果画面を出力し(ステップS213)、ステップS205に戻り処理を続ける。

#### 【0047】

##### <コンテンツインデックス出力プログラム>

図10は、コンテンツインデックス出力プログラムの動作を示すフローチャートである。コンテンツインデックス出力プログラムは、復号鍵要求プログラムのステップS205の詳細である。

コンテンツインデックス画面制御を読み出し(ステップS301)、インデックス復号鍵情報を読み出す(ステップS302)。続いて、インデックス復号鍵情報を用いてコンテンツインデックス画面制御情報を復号する(ステップS303)。復号したコンテンツインデックス画面制御情報からコンテンツインデックス画面を生成し、生成したコンテンツインデックス画面を出力する(ステップS304)。

#### 【0048】

##### 3. ユーザ用クライアント30

ここでは、ユーザ用クライアント30の構成について説明する。

図9は、ユーザ用クライアント30の構成を示すブロック図である。同図に示す様に、ユーザ用クライアント30は、送受信部301、入力部302、表示部303、制御部304、復号部305、入出力部306及びプログラム記憶部307から構成される。制御部304は、読出部304a、解読部304b及び実行部304cを含む。

#### 【0049】

ユーザ用クライアント30は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード及びマウスなどから構成されるコンピュータシステムであり、ここでは特にパーソナルコンピュータを想定している。

(1) 送受信部301

送受信部301は、イントラネット60を介して制御部304の実行部304cとコンテンツ管理サーバ10との間で情報の送受信を行う。具体的には、送受信部301は、ユーザID、パスワード、コンテンツID等をコンテンツ管理サーバ10へ送信し、コンテンツ管理サーバ10から復号鍵等を受信する。

【0050】

(2) 入力部302

入力部302は、具体的にはキーボード及びマウス等のユーザインターフェースユニットである。キーボード及びマウスがユーザにより操作されると、入力部302は、操作に相当する操作指示を、制御部304の実行部304cを介して送受信部301及び表示部303へ出力する。

【0051】

(3) 表示部303

表示部303は、ディスプレイユニットを備え、実行部304cから画面データを受け取り、受け取った画面データをディスプレイユニットに表示する。また、表示部303は、入力部302が受け付けた操作指示に応じた入力情報を、実行部304cを介してディスプレイユニットに表示する。表示部303が表示する画面は、ユーザ認証画面310、コンテンツインデックス画面320、コンテンツ検索画面410、検索結果画面510、復号確認画面610及び復号結果画面710である。更に、表示部303は、制御部304から、復号部305が復号したコンテンツを受け取り、受け取ったコンテンツをディスプレイユニットに表示する。

【0052】

以下、各画面について説明する。

(ユーザ認証画面310)

ユーザ認証画面 3 1 0 は、各利用者が当該システムの利用を開始する都度、必ず表示される画面であり、図 1 0 示す様に、ユーザ ID 記入欄 3 1 1、パスワード記入欄 3 1 2、OK ボタン 3 1 3 及びキャンセルボタン 3 1 4 を備える。

## 【 0 0 5 3 】

表示部 3 0 3 は、ユーザ ID 記入欄 3 1 1 において入力部 3 0 2 により入力を受け付けた情報を受け取り、受け取った情報をユーザ ID 記入欄 3 1 1 に表示する。パスワード記入欄 3 1 2 においても同様である。また、OK ボタン 3 1 3 又はキャンセルボタン 3 1 4 において、利用者からマウスの操作による入力を受け付けると、操作に対応した指示を制御部 3 0 4 の実行部 3 0 4 c へ出力する。

## 【 0 0 5 4 】

(コンテンツインデックス画面 3 2 0)

コンテンツインデックス画面 3 2 0 は、コンテンツ管理サーバ 1 0 がユーザ認証に成功した場合に、表示部 3 0 3 に表示される画面であり、図 1 1 に示す様に、コンテンツインデックス 3 2 1、復号ボタン 3 2 2、終了ボタン 3 2 3 及び検索ボタン 3 2 4 を備える。

## 【 0 0 5 5 】

コンテンツインデックス 3 2 1 は、記録媒体 2 0 に格納されている暗号化コンテンツインデックス 2 0 2 が復号化されたものである。コンテンツインデックス 3 2 1 は、右端にスクロールバー及びスクロールボタンを有する。表示部 3 0 3 は、入力部 3 0 2 によりスクロールバー及びスクロールボタンが操作されると、コンテンツインデックス 3 2 1 をスクロールして表示する。表示部 3 0 3 は、コンテンツインデックス 3 2 1 の一のコンテンツ上においてマウスのクリックによる入力を受け付けると、当該コンテンツが選択されたことを示す反転表示をコンテンツインデックス 3 2 1 に表示する。

## 【 0 0 5 6 】

復号ボタン 3 2 2 は、選択されたコンテンツの復号を要求するために用いられるボタンである。終了ボタン 3 2 3 は、コンテンツインデックス画面 3 2 0 の表示を終了することを要求するために用いられるボタンである。検索ボタン 3 2 4 は、コンテンツの検索を要求するために用いられるボタンである。



## (コンテンツ検索画面 4 1 0)

コンテンツ検索画面 4 1 0 は、コンテンツインデックス画面 3 2 0 において、入力部 3 0 2 が検索ボタン 3 2 4 の選択を受け付けた際に表示される画面である。

## 【 0 0 5 7 】

図 1 2 に示す様に、コンテンツ検索画面 4 1 0 は、コンテンツ I D 記入欄 4 1 1、キーワード記入欄 4 1 2、作成者記入欄 4 1 3、分野記入欄 4 1 4、検索方法選択欄 4 1 5 検索ボタン 4 1 6、クリアボタン 4 1 7 及びキャンセルボタン 4 1 8 を備える。

表示部 3 0 3 は、コンテンツ I D 記入欄 4 1 1 において、入力部 3 0 2 により入力が受け付けられた情報を受け取り、受け取った情報をコンテンツ I D 記入欄 4 1 1 に表示する。キーワード記入欄 4 1 2、作成者記入欄 4 1 3 及び分野記入欄 4 1 4 においても同様である。検索方法選択欄 4 1 5 は、2 つのラジオボタンを有し、各ラジオボタンは、AND 検索又は OR 検索を選択するために用いられる。表示部 3 0 3 は、各ラジオボタンにおいて、入力部 3 0 2 から操作指示を受けると、選択された状態を示すマークをラジオボタンに表示する。なお、検索方法選択欄 4 1 5 において、ラジオボタンは、何れか 1 つが選択されると他が選択解除される。

## 【 0 0 5 8 】

検索ボタン 4 1 6 は、入力された条件においての検索を要求するために用いられるボタンである。クリアボタン 4 1 7 は、入力されたコンテンツ I D、キーワード等の検索条件の破棄を要求するために用いられるボタンである。キャンセルボタン 4 1 8 は、コンテンツ検索の終了を要求するために用いられるボタンである。

## 【 0 0 5 9 】

## (検索結果画面 5 1 0)

検索結果画面 5 1 0 は、コンテンツ検索画面 4 1 0 において、検索条件が入力され、且つ、入力部 3 0 2 が検索ボタン 4 1 6 の選択を受け付けた場合に表示される画面である。図 1 3 に示す様に、検索結果画面 5 1 0 は、メッセージ表示部

5 1 1、コンテンツインデックス 5 1 2、復号ボタン 5 1 3、終了ボタン 5 1 4、検索ボタン 5 1 5 及び全件表示ボタン 5 1 6 を備える。

【 0 0 6 0 】

メッセージ表示部 5 1 1 は、「検索結果：〇件ヒットしました。」というメッセージにより、検索により得られたコンテンツの件数を表示する。コンテンツインデックス 5 1 2 は、検索の結果得られた全てのコンテンツについて、コンテンツ毎に分野、コンテンツ ID、作成者及び文書インデックスを記述したものである。コンテンツインデックス 5 1 2 は、右端にスクロールバー及びスクロールボタンを有する。表示部 3 0 3 は、入力部 3 0 2 によりスクロールバー及びスクロールボタンが操作されると、コンテンツインデックス 5 1 2 をスクロールして表示する。表示部 3 0 3 は、コンテンツインデックス 5 1 2 の一のコンテンツ上においてマウスのクリックによる入力を受け付けると、当該コンテンツが選択されたことを示す反転表示をコンテンツインデックス 5 1 2 に表示する。

【 0 0 6 1 】

復号ボタン 5 1 3 は、選択されたコンテンツの復号を要求するために用いられるボタンである。終了ボタン 5 1 4 は、検索結果画面 5 1 0 の表示を終了することを要求するために用いられるボタンである。検索ボタン 5 1 5 は、再度コンテンツの検索を要求するために用いられるボタンである。全件表示ボタン 5 1 6 は、記録媒体 2 0 に格納されている全てのコンテンツについてのコンテンツインデックスの表示を要求するために用いられるボタンであり、具体的には、入力部 3 0 2 が全件表示ボタン 5 1 6 の選択を受け付けると、表示部 3 0 3 は、前述したコンテンツインデックス画面 3 2 0 を表示する。

【 0 0 6 2 】

(復号確認画面 6 1 0)

復号確認画面 6 1 0 は、前述したコンテンツインデックス画面 3 2 0、又は、検索結果画面 5 1 0 において、コンテンツの選択がなされ、且つ、入力部 3 0 2 が復号ボタン 3 2 2、又は、復号ボタン 5 1 3 の選択を受け付けた場合に表示される画面である。復号確認画面 6 1 0 は、図 1 4 に示す様に、メッセージ表示部 6 1 1、選択コンテンツ表示部 6 1 2、OK ボタン 6 1 3 及びキャンセルボタン

6 1 4 を備える。

【 0 0 6 3 】

メッセージ表示部 6 1 1 は、「選択されたコンテンツは下記の通りです。」というメッセージを表示する。復号結果表示部 7 1 2 は、選択コンテンツ表示部 6 1 2 は、コンテンツインデックス画面 3 2 0、又は、検索結果画面 5 1 0 において、復号化が要求された全てのコンテンツについて、コンテンツ毎に、分野、コンテンツ ID 及び文書インデックスが表示される。復号確認画面 6 1 0 において、OK ボタン 6 1 3、又は、キャンセルボタン 6 1 4 において、利用者からマウスの操作による入力を受け付けると、操作に対応した指示を制御部 3 0 4 の実行部 3 0 4 c へ出力する。

【 0 0 6 4 】

(復号結果画面 7 1 0)

復号結果画面 7 1 0 は、前述した復号確認画面 6 1 0 において、入力部 3 0 2 が OK ボタン 6 1 3 の選択を受け付けた場合に表示される画面である。復号結果画面 7 1 0 は、図 1 5 に示す様に、メッセージ表示部 7 1 1、復号結果表示部 7 1 2、OK ボタン 7 1 3 及びキャンセルボタン 7 1 4 を備える。

【 0 0 6 5 】

メッセージ表示部 7 1 1 は、「復号化の結果は以下の通りです。」というメッセージを表示する。復号結果表示部 7 1 2 は、復号化が要求されたコンテンツについて、コンテンツ ID と復号結果とを表示する。復号結果は例として、「成功しました」、「公開時間外です」等である。復号結果画面 7 1 0 において、OK ボタン 7 1 3、又は、キャンセルボタン 7 1 4 において、利用者からマウスの操作による入力を受け付けると、操作に対応した指示を制御部 3 0 4 の実行部 3 0 4 c へ出力する。

【 0 0 6 6 】

(4) 制御部 3 0 4

制御部 3 0 4 は、読出部 3 0 4 a、解読部 3 0 4 b 及び実行部 3 0 4 c を含み、具体的には、マイクロプロセッサ及び RAM 等から構成される。前記 RAM は、制御用コンピュータプログラムを記憶し、前記マイクロプロセッサが前記制御

用コンピュータプログラムを実行することにより、制御部 3 0 4 は、ユーザ用クライアント 3 0 全体を制御する。

【 0 0 6 7 】

制御部 3 0 4 は、入力部 3 0 2 から受け取る入力情報に基づいて、送信情報を生成し、生成した送信情報を送受信部 3 0 1 及びイントラネット 6 0 を介して、コンテンツ管理サーバ 1 0 のゲートウェイ 1 0 1 へ送信すると共に、前記入力情報を表示部 3 0 3 へ出力する。

制御部 3 0 4 は、イントラネット 6 0 及び送受信部 3 0 1 を介して、コンテンツ管理サーバ 1 0 から受信する受信情報に基づいて出力情報を生成し、生成した出力情報を表示部 3 0 3 に出力する。更に、制御部 3 0 4 は、イントラネット 6 0 及び送受信部 3 0 1 を介して、コンテンツ管理サーバ 1 0 から受信する復号鍵を復号部 3 0 5 へ出力する。

【 0 0 6 8 】

また、制御部 3 0 4 は、入出力部 3 0 6 に記録媒体 2 0 が装着された状態において、どのプログラムを讀出して実行するかを選択するプログラムの実行中に、ユーザの入力により、記録媒体 2 0 に格納されている復号鍵要求プログラム及びコンテンツインデックス出力プログラムを実行する要求を受け付けると、以下に示す様にして記録媒体 2 0 に格納されたプログラムを実行する。

【 0 0 6 9 】

先ず、読出部 3 0 4 a は、入出力部 3 0 6 に対して記録媒体 2 0 に格納されている復号鍵要求プログラム、コンテンツインデックス出力プログラム、暗号化コンテンツインデックス、インデックス復号鍵情報及び画面制御情報を読み出し、読み出した復号鍵要求プログラム、コンテンツインデックス出力プログラム、暗号化コンテンツインデックス、インデックス復号鍵情報及び画面制御情報をプログラム記憶部 3 0 7 に書き込む指示を出力する。プログラム記憶部 3 0 7 に上記プログラム及び上記データが書き込まれると、読出部 3 0 4 a は、プログラム記憶部 3 0 7 からプログラムを順に読み出し、読み出したプログラムを解読部 3 0 4 b が解読し、解読したプログラムを実行部 3 0 4 c が実行する。

【 0 0 7 0 】

具体的には、復号鍵要求処理においては、実行部 3 0 4 c は、画面制御情報に基づき、画面データを生成し、生成した画面データを表示部 3 0 3 へ出力する。実行部 3 0 4 c は、入力部 3 0 2 を介してコンテンツの選択及び復号化を要求する入力を受け付け、受け付けた入力に対応するコンテンツ ID と入力した利用者を示すユーザ ID とを送受信部 3 0 1 に出力する。コンテンツインデックス復号処理においては、実行部 3 0 4 c は、インデックス復号鍵情報を用いて暗号化コンテンツインデックスを復号する。

## 【 0 0 7 1 】

実行部 3 0 4 c は、プログラム記憶部 3 0 7 に格納されたプログラムを全て実行すると、プログラム記憶部 3 0 7 に対して、格納しているプログラム及びデータを全て破棄する指示を出力し、プログラム記憶部 3 0 7 は、プログラム及びデータを破棄する。

## ( 5 ) 復号部 3 0 5

復号部 3 0 5 は、マイクロプロセッサ及び RAM 等から構成される。前記 RAM は、復号化プログラムを記憶し、前記マイクロプロセッサが前記復号化プログラムを実行することにより復号部 3 0 5 は暗号化コンテンツを復号する。

## 【 0 0 7 2 】

復号部 3 0 5 は、制御部 3 0 4 から復号鍵を受け取り、受け取った復号鍵に base 6 4 変換の逆変換を施す。制御部 3 0 4 は、入出力部 3 0 6 が記録媒体 2 0 から読み出した暗号化コンテンツに、base 6 4 変換の逆変換を施した復号鍵を用いて、復号アルゴリズム  $D_1$  を施して復号する。ここで、復号アルゴリズム  $D_1$  は、暗号アルゴリズム  $E_1$  により生成された暗号文を復号するアルゴリズムである。また、復号部 3 0 5 は、復号したコンテンツを制御部 3 0 4 に出力する。

## 【 0 0 7 3 】

## ( 6 ) 入出力部 3 0 6

入出力部 3 0 6 は、具体的には CD-ROM ドライブユニットであり、CD-ROM である記録媒体 2 0 が装着された状態において、記録媒体 2 0 に格納されている復号鍵要求プログラム、コンテンツインデックス出力プログラム、暗号化

コンテンツインデックス、インデックス復号鍵情報及び画面制御情報を読み出して、プログラム記憶部 3 0 7 に出力する。

【 0 0 7 4 】

また、入出力部 3 0 6 は、制御部 3 0 4 が、コンテンツ管理サーバから復号鍵を受信すると、記録媒体 2 0 に格納されている暗号化コンテンツを読み出して、制御部 3 0 4 へ出力する。

( 7 ) プログラム記憶部 3 0 7

プログラム記憶部 3 0 7 は、具体的には R A M であり、入出力部 3 0 6 が記録媒体 2 0 から読み出す復号鍵要求プログラム、コンテンツインデックス出力プログラム、暗号化コンテンツインデックス、インデックス復号鍵情報及び画面制御情報を一時的に格納する。プログラム記憶部 3 0 7 は、復号鍵要求プログラムとコンテンツインデックス出力プログラムとの実行処理が終了すると、格納している上記プログラム及びデータを全て破棄する。

【 0 0 7 5 】

4 . 管理者用クライアント 4 0

管理者用クライアント 4 0 は、コンテンツ管理システム 1 の管理者が有する装置である。管理者用クライアントは、具体的にはパーソナルコンピュータである。管理者用クライアント 4 0 は、ユーザ用クライアント 3 0 と同様の構成を有するため図示していない。

【 0 0 7 6 】

管理者用クライアント 4 0 は、管理者の操作による入力を受け付けると、コンテンツ管理サーバ 1 0 へ履歴情報を要求する信号を送信し、コンテンツ管理サーバ 1 0 から、履歴情報を受信する。更に、管理者用クライアント 4 0 は、管理者の操作による入力を受け付けると、コンテンツ管理サーバ 1 0 のデータベース部 1 0 2 に格納されている各データを更新する。詳細は後述する。

【 0 0 7 7 】

5 . 提供者用クライアント 5 0

提供者用クライアント 5 0 は、記録媒体 2 0 に格納されているコンテンツの提供者が有する装置であって、具体的にはパーソナルコンピュータである。提供者

用クライアント50は、ユーザ用クライアント30と同様の構成を有するため図示していない。提供者用クライアント50は、提供者の操作による入力を受け付けると、コンテンツ管理サーバ10へ履歴情報を要求する信号を送信し、コンテンツ管理サーバ10から、履歴情報を受信する。詳細は後述する。

#### 【0078】

##### <動作>

ここでは、コンテンツ管理システム1の動作について、図面を参照して説明する。

##### 1. 全体の動作

コンテンツ管理システム1における全ての処理は、図18のフローチャートに示す様に、マイクロプロセッサがコンピュータプログラムを読み出し（ステップS501）、読み出したコンピュータプログラムを解読し（ステップS502）、解読したコンピュータプログラムを実行する（ステップS503）ことにより実現される。

#### 【0079】

図19は、コンテンツ管理システム1の全体の動作を示すフローチャートである。

ユーザ用クライアント30は、記録媒体20に格納されている鍵要求プログラムを読み出す（ステップS601）。ユーザ用クライアント30は、読み出した鍵要求プログラムを実行する（ステップS602）。続いて、ユーザ用クライアント30はコンテンツ管理サーバ10に対してコンテンツの復号鍵を要求する信号を送信し、コンテンツ管理サーバ10は、信号を受信する（ステップS603）。コンテンツ管理サーバ10は、要求に応じた処理を行う（ステップS604）。コンテンツ管理サーバ10は、ユーザ用クライアント30へ復号鍵又はエラーメッセージを送信し、ユーザ用クライアント30は、復号鍵又はエラーメッセージを受信する（ステップS605）。復号鍵を受信した場合（ステップS606でYES）、ユーザ用クライアント30は、記録媒体20から暗号化コンテンツを読み出し（ステップS607）、読み出した暗号化コンテンツを復号鍵を用いて復号する（ステップS608）。ユーザ用クライアント30は、復号したコ

ンテンツ又はエラーメッセージを表示するステップS 6 0 9)。

【0 0 8 0】

提供者用クライアント5 0は、情報提供の要求を示す信号をコンテンツ管理サーバ1 0へ送信し、コンテンツ管理サーバ1 0は、信号を受信する(ステップS 6 1 1)。コンテンツ管理サーバ1 0は、要求に応じた処理を行う(ステップS 6 1 2)。コンテンツ管理サーバ1 0は、提供者用クライアント5 0へ履歴情報を送信し、提供者用クライアント5 0は、履歴情報を受信する(ステップS 6 1 3)。

【0 0 8 1】

管理者用クライアント4 0は、情報提供の要求を示す信号をコンテンツ管理サーバ1 0へ送信し、コンテンツ管理サーバ1 0は、信号を受信する(ステップS 6 2 2)。コンテンツ管理サーバ1 0は、要求に応じた処理を行う(ステップS 6 2 3)。コンテンツ管理サーバ1 0は、履歴情報を管理者用クライアント4 0へ送信し、管理者用クライアント4 0は、履歴情報を受信する(ステップS 6 2 3)。更に、管理者用クライアント4 0は、更新の要求を示す信号をコンテンツ管理サーバ1 0へ送信し、コンテンツ管理サーバ1 0は信号を受信する(ステップS 6 2 4)。コンテンツ管理サーバ1 0は、要求に応じた処理を行う(ステップS 6 2 5)。

【0 0 8 2】

2. コンテンツ管理サーバ1 0の動作

ここでは、コンテンツ管理サーバ1 0の動作について説明する。

図2 0に示すフローチャートは、図1 9に示したフローチャートにおける、ステップS 6 0 4、ステップS 6 1 2、ステップS 6 2 2及びステップS 6 2 5における動作の詳細である。

【0 0 8 3】

コンテンツ管理サーバ1 0は、受信した信号が示す要求の種類を判断する(ステップS 1 0 1)。受信した信号が「コンテンツ開示」を要求するものであれば(ステップS 1 0 2で「開示」)、鍵送信の判断処理を行う(ステップS 1 0 3)。受信した信号が「提供者への情報提供を」を要求するものであれば(ステッ



プ S 1 0 2 で「提供者」)、提供者への情報提供の処理を行う(ステップ S 1 0 4)。受信した信号が「管理者への情報提供」を要求するものであれば(ステップ S 1 0 2 で「管理者」)、履歴管理部 1 0 4 は、データベース部 1 0 2 に格納されている履歴テーブル 1 5 0 に含まれる全ての履歴情報を読み出す(ステップ S 1 0 5)。受信した信号が「データの更新」を要求するものであれば(ステップ S 1 0 2 で「更新」)、データの更新の処理を行う(ステップ S 1 0 6)。

#### 【 0 0 8 4 】

### 3. 鍵送信判断処理の動作

図 2 1 は、鍵送信判断処理の動作を示すフローチャートである。ここで説明する動作は、図 2 0 のフローチャートにおけるステップ S 1 0 3 の詳細である。

コンテンツ管理サーバ 1 0 のユーザ認証部 1 0 3 は、ゲートウェイ 1 0 1 を介してコンテンツ ID 及びユーザ ID を受信し、受信したコンテンツ ID 及びユーザ ID を記憶する(ステップ S 4 0 2)。ユーザ認証部 1 0 3 は、履歴情報を生成し、生成した履歴情報をデータベース部 1 0 2 の履歴テーブル 1 5 0 に追加する(ステップ S 4 0 3)。

#### 【 0 0 8 5 】

ユーザ認証部 1 0 3 は、データベース部 1 0 2 に格納されている履歴テーブル 1 5 0 を用いて、当該ユーザが既に利用したコンテンツの累積件数を計数する。ユーザ認証部 1 0 3 は、前記ユーザ ID と同じユーザ ID を含むユーザ情報をデータベース部 1 0 2 のユーザテーブル 1 2 0 から読み出す(ステップ S 4 0 4)。ユーザ認証部 1 0 3 は、計数した累積件数と読み出したユーザ情報に含まれる利用可能件数とを比較して利用許可件数の判断を行う(ステップ S 4 0 5)。利用許可件数が累積件数以下である場合(ステップ S 4 0 6 で「NO」)、ユーザ認証部 1 0 3 は、既に利用許可件数を超過していることを通知するエラーメッセージを出力し(ステップ S 4 0 7)、処理を続ける。利用許可件数が累積件数より大きい場合(ステップ S 4 0 6 で「YES」)、ユーザ認証部 1 0 3 は、前記コンテンツ ID と同じコンテンツ ID を含むコンテンツ情報をデータベース部 1 0 2 のコンテンツテーブル 1 3 0 から読み出す(ステップ S 4 0 8)。

#### 【 0 0 8 6 】

ユーザ認証部 1 0 3 は、読み出したコンテンツ情報に含まれる公開可能期間（開始）及び公開可能期間（終了）を読み、現在が公開期間であるか判断する（ステップ S 4 0 9）。現在が公開期間でない場合（ステップ S 4 1 0 で「NO」）、ユーザ認証部 1 0 3 は、公開期間でないことを通知するエラーメッセージを出力し（ステップ S 4 1 1）、処理を続ける。現在が公開期間である場合（ステップ S 4 1 0 で「YES」）、ユーザ認証部 1 0 3 は、記憶した前記ユーザ情報に含まれる利用可能公開区分と前記コンテンツ情報に含まれる公開区分とを読み、公開区分の判断を行う（ステップ S 4 1 2）。前記利用可能公開区分が前記公開区分を含まない場合（ステップ S 4 1 3 で「NO」）、ユーザ認証部 1 0 3 は、当該コンテンツは、当該ユーザの利用可能な公開区分に含まれないことを示すエラーメッセージを出力し（ステップ S 4 1 4）、処理を続ける。前記利用可能公開区分が前記公開区分を含む場合（ステップ S 4 1 3 で「YES」）、ユーザ認証部 1 0 3 は、データベース部 1 0 2 の複号鍵テーブル 1 4 0 から、当該コンテンツに対応する複号鍵情報を読み出す（ステップ S 4 1 5）。

#### 【 0 0 8 7 】

#### 4. 提供者への情報提供処理の動作

図 2 2 は、提供者への情報提供の処理におけるコンテンツ管理サーバ 1 0 と提供者用クライアント 5 0 の動作を示すフローチャートである。なお、ここで示す動作は、図 2 0 に示したフローチャートのステップ S 1 0 4 の詳細である。

提供者用クライアント 5 0 は、当該提供者のユーザ ID の入力を受け付ける（ステップ S 7 0 1）。提供者用クライアント 5 0 は、受け付けたユーザ ID を、イントラネット 6 0 を介してコンテンツ管理サーバ 1 0 へ送信し、コンテンツ管理サーバ 1 0 はユーザ ID を受信する（ステップ S 7 0 2）。次に、コンテンツ管理サーバ 1 0 の履歴管理部 1 0 4 は、データベース部 1 0 2 のコンテンツテーブル 1 3 0 から、受信したユーザ ID を含む全てのコンテンツ情報に含まれるコンテンツ ID を読み出す（ステップ S 7 0 3）。続いて、履歴管理部 1 0 4 は、データベース部 1 0 2 の履歴テーブル 1 5 0 から、読み出したコンテンツ ID を含む全ての履歴情報を読み出す（ステップ S 7 0 4）。履歴管理部 1 0 4 は、ゲートウェイ 1 0 1 及びイントラネット 6 0 を介して、読み出した履歴情報を提供

者用クライアント 5 0 へ送信し、提供者用クライアント 5 0 は、履歴情報を受信する（ステップ S 7 0 5）。提供者用クライアント 5 0 は、受信した履歴情報をディスプレイユニットに表示する（ステップ S 7 0 6）。

#### 【 0 0 8 8 】

##### 5. データ更新処理の動作

図 2 3 は、コンテンツ管理サーバ 1 0 のデータベース部 1 0 2 に格納されているデータのデータ更新処理におけるコンテンツ管理サーバ 1 0 と管理者用クライアント 4 0 の動作を示すフローチャートである。

管理者用クライアント 4 0 は、コンテンツ ID の入力を受け付ける（ステップ S 8 0 1）。管理者用クライアント 4 0 は、受け付けたコンテンツ ID をイントラネット 6 0 を介してコンテンツ管理サーバ 1 0 へ送信し、コンテンツ管理サーバはコンテンツ ID を受信する（ステップ S 8 0 2）。コンテンツ管理サーバ 1 0 のデータベース管理部 1 0 5 は、データベース部 1 0 2 のコンテンツテーブル 1 3 0 から、受信したコンテンツ ID を含むコンテンツ情報を読み出す（ステップ S 8 0 3）。データベース管理部 1 0 5 は、読み出したコンテンツ情報をゲートウェイ 1 0 1 及びイントラネット 6 0 を介して管理者用クライアント 4 0 へ送信し、管理者用クライアント 4 0 は、コンテンツ情報を受信する（ステップ S 8 0 4）。管理者用クライアント 4 0 は、受信したコンテンツ情報をディスプレイユニットに表示し（ステップ S 8 0 5）、更新するデータの入力を受け付ける（ステップ S 8 0 6）。管理者用クライアント 4 0 は、受け付けた更新データをイントラネット 6 0 及びゲートウェイ 1 0 1 を介してコンテンツ管理サーバ 1 0 のデータベース管理部 1 0 5 へ送信し、データベース管理部 1 0 5 は、更新データを受信する（ステップ S 8 0 7）。続いて、データベース管理部 1 0 5 は、受信した更新データに基づき、対応するデータを更新する（ステップ S 8 0 8）。

#### 【 0 0 8 9 】

##### < まとめ >

以上説明したように、本発明は、記録媒体 2 0 に格納されて利用者に配布された暗号化コンテンツについて、コンテンツに係る情報と利用者に係る情報とをコンテンツ管理サーバ 1 0 が管理することにより公開期間、公開区分等に応じてコ

ンテンツの開示を制御する。

【 0 0 9 0 】

本発明は、管理者の要求を受けてコンテンツ管理サーバ 1 0 が、コンテンツ情報、利用者情報等に含まれる各項目を変更することが可能であり、更に、データを変更すると直ちに変更後のデータで開示の制御が可能であり、コンテンツの開示を動的にきめ細かく管理するシステムである。

また、コンテンツの開示が要求されたコンテンツ及び当該コンテンツを要求した利用者の情報を蓄積して管理する。

【 0 0 9 1 】

更に、暗号化コンテンツの復号鍵を要求するためのコンピュータプログラムは、暗号化コンテンツと共に記録媒体 2 0 に格納されており、ユーザ用クライアント 3 0 の制御部 3 0 4 が記録媒体 2 0 に格納されているコンピュータプログラムを読み出して実行することにより、復号鍵要求処理が実現される。

<その他の変形例>

( 1 ) 上記実施の形態では、コンテンツ管理システム 1 を構成するコンテンツ管理サーバ 1 0 、ユーザ用クライアント 3 0 、管理者用クライアント 4 0 及び提供者用クライアント 5 0 がイントラネット 6 0 を介して接続されているが、上記の装置が、インターネットを介して接続されて構成されるシステムも本発明に含まれる。

【 0 0 9 2 】

更に、上記実施の形態におけるコンテンツとは、企業が管理している P D F ファイル形式の技術資料であったが、本発明のコンテンツはこれに限定されないのは勿論である。コンテンツは、文字データ、音楽データ、画像データ、動画データ等デジタルデータであればよい。

( 2 ) 上記実施の形態では、ユーザ用クライアント 3 0 及び提供者用クライアント 5 0 は、それぞれ 1 ずつであるが、複数のユーザ用クライアント及び提供者用クライアントが、コンテンツ管理サーバ 1 0 と相互にイントラネットを介して接続された構成も本発明に含まれる。

【 0 0 9 3 】

(3) 上記実施の形態では、CD-ROMに暗号化コンテンツ、各コンピュータプログラム及び各データが格納されているが、本発明で用いる記録媒体は、CD-ROMに限定されないのは勿論である。フレキシブルディスク、MO、DVD-ROM、DVD-RAM等コンピュータ読取可能な他の記録媒体に格納する構成としてもよい。

【0094】

(4) コンテンツ管理システム1の管理者及びコンテンツを作成した提供者もユーザID及びパスワードを有し、記録媒体に格納された暗号化コンテンツの配布を受けて、コンテンツの利用が可能である構成も本発明に含まれる。

(5) 上記実施の形態では、データ更新の処理においてコンテンツ情報を更新しているが、更新が可能な情報はコンテンツ情報に限定されない。データベース部102に格納されている情報のうち、ユーザ認証情報、ユーザ情報、コンテンツ情報及び復号鍵情報は更新が可能である。これらの情報を更新する構成も本発明に含まれる。

【0095】

(6) 上記実施の形態では、コンテンツ管理サーバ10からユーザ用クライアント30へ送信される復号鍵は、コンテンツ管理サーバ10でbase64変換を施した後イントラネット60を介してユーザ用クライアント30へ送信される構成としているが、コンテンツ管理サーバ10が復号鍵を秘密鍵暗号方式、又は公開鍵暗号方式により暗号化した後にイントラネット60を介してユーザ用クライアント30へ送信する構成としてもよい。この場合、ユーザ用クライアント30は、秘密鍵暗号化方式で暗号化された復号鍵を取得すると、

(7) 上記実施の形態において、記録媒体20に格納されている鍵要求プログラム及びコンテンツインデックス出力プログラムは、ユーザ用クライアント30にインストールすることができず、ユーザ用クライアント30の制御部304が記録媒体20から読み出して実行することによってのみコンテンツ管理サーバ10に対して復号鍵を要求することができる。更に、鍵要求プログラム及びコンテンツインデックス出力プログラムは、ライセンスを有する真正な利用者のみ、ユーザ用クライアント30を用いて読み出すことが可能である。そのため、記録媒

体 2 0 に格納されている全てのデータ及びプログラムが記録媒体又は H D D にコピーされた場合であっても、復号鍵を要求するための用いる鍵要求プログラム及びコンテンツインデックスプログラムを読み出すことはできず、鍵を取得することは不可能であるため、暗号化コンテンツを安全に管理することができる。

## 【 0 0 9 6 】

( 8 ) 上記実施の形態では、ユーザ用クライアント 3 0 が鍵要求プログラムを実行することにより暗号化コンテンツの復号鍵をコンテンツ管理サーバ 1 0 に要求すると当該利用者の履歴情報が生成されて履歴テーブルに追加される構成としているが、コンテンツ管理サーバ 1 0 が復号鍵を送信した利用者の履歴情報を生成して履歴テーブルに追加する構成としてもよい。

## 【 0 0 9 7 】

( 9 ) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、C D - R O M 、 M O 、 D V D - R O M 、 D V D - R A M 、半導体メモリ等に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は、前記デジタル信号を電気通信回路、無線又は有線通信回路、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

## 【 0 0 9 8 】

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、前記コンピュータプログラムを記憶しており、前記マイクロプロセッサが前記コンピュータプログラムに従って動作するとしてもよい。

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は、前記プログラム又は前記デジタル信号を、ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより

実施するとしてもよい。

【0099】

(10) 上記実施の形態及び上記変形例を組み合わせてもよい。

【0100】

【発明の効果】

以上説明したように、本発明は、可搬型の記録媒体に格納された暗号化コンテンツを、管理装置から取得した復号鍵を用いて再生装置により再生するコンテンツ管理システムであって、前記管理装置は、前記暗号化コンテンツを復号する為の復号鍵と前記暗号化コンテンツの開示の可否を示す開示情報とを対応付けて保持しており、前記記録媒体は、暗号鍵を用いて暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求する鍵要求プログラムとを格納しており、前記再生装置は、前記記録媒体から前記鍵要求プログラムを読み出して実行し、前記管理装置は、前記再生装置からの要求を受けると、前記暗号化コンテンツの開示の可否を前記開示情報に応じて判断し、開示可と判断した場合に前記復号鍵を前記再生装置へ送信し、前記再生装置は、前記管理装置から前記復号鍵を受信し、前記記録媒体から前記暗号化コンテンツを読み出して前記復号鍵を用いて復号し再生することを特徴とする。

【0101】

この構成によると、暗号化コンテンツの開示の可否を示す開示情報が管理装置に保持されているため、可搬型の記録媒体を利用者に配布した後であっても、開示情報を管理装置が一元的に管理することが可能である。さらに、管理装置に対して復号鍵を要求するために用いられる鍵要求プログラムが記録媒体に格納されていることにより、開示情報が記録媒体に格納されている場合と同様にコンテンツを安全に管理することができる、

ここで、前記再生装置は、前記記録媒体から前記鍵要求プログラムを読み出して解読し実行する鍵要求プログラム実行手段と、前記管理装置から前記復号鍵を受信する復号鍵受信手段と、前記記録媒体から前記暗号化コンテンツを読み出すコンテンツ読出手段と、前記復号鍵を用いて前記暗号化コンテンツを復号し再生する再生手段とを備え、前記管理装置は、前記暗号化コンテンツを復号する為の

復号鍵を記憶している鍵記憶手段と、前記暗号化コンテンツの開示の可否を示す開示情報を記憶している開示情報記憶手段と、前記再生装置からの要求を受けて、前記開示情報に応じて前記暗号化コンテンツの開示の可否を判断する開示判断手段と、開示可と判断した場合に、前記復号鍵を前記再生装置へ送信する復号鍵送信手段とを備えるように構成してもよい。

## 【 0 1 0 2 】

この構成によると、再生装置が記録媒体に格納されている鍵要求プログラムを読み出すことにより、管理装置に対して暗号化コンテンツを復号する為に用いる復号鍵を要求するため、記録媒体の配布を受けた真正な利用者のみが復号鍵を要求することができ、コンテンツを安全に管理することができる。

また、本発明は、管理装置から取得する復号鍵を用いて再生装置により再生される暗号化コンテンツを格納した可搬型の記録媒体であって、前記管理装置は、前記暗号化コンテンツの復号鍵を保持しており、前記記録媒体は、暗号鍵により暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求するための鍵要求プログラムとを格納していることを特徴とする。

## 【 0 1 0 3 】

この構成によると、記録媒体は、暗号化コンテンツの開示を制限する開示情報を格納していないが、暗号化コンテンツを復号する為の復号鍵を要求するための鍵要求プログラムを格納しているため、コンテンツの安全性を保つことができる。

また、本発明は、可搬型の記録媒体に格納された暗号化コンテンツを復号する為の復号鍵を保持し、前記復号鍵を再生装置に送信する管理装置であって、前記記録媒体は、暗号鍵を用いて暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求する鍵要求プログラムとを格納しており、前記管理装置は、前記暗号化コンテンツを復号する為の復号鍵を記憶している鍵記憶手段と、前記暗号化コンテンツの開示の可否を示す開示情報を記憶している開示情報記憶手段と、前記再生装置からの要求を受けて、前記開示情報に応じて前記暗号化コンテンツの開示の可否を判断する開示判断手段と、開示可と判断した場合に、前記復号鍵を前記再生装置へ送信する復号鍵送信手段とを備えることを特徴とする。



## 【 0 1 0 4 】

この構成によると、管理装置は、可搬型の記録媒体に格納された暗号化コンテンツを復号する為の復号鍵と暗号化コンテンツの開示の可否を示す開示情報とを記憶しているため、暗号化コンテンツの開示の可否を、管理装置が一元管理することができる。

ここで、前記開示情報記憶手段は、前記記録媒体及び前記再生装置を有する利用者を識別する利用者識別子を含み、前記利用者識別子により識別される利用者に対する前記暗号化コンテンツの開示の可否を示す開示情報を記憶しており、前記開示判断手段は、前記再生装置から前記利用者識別子を含む要求を受け付けると、前記開示情報を用いて、前記利用者識別子により識別される利用者に対する前記暗号化コンテンツの開示の可否を判断するように構成してもよい。

## 【 0 1 0 5 】

この構成によると、管理装置が利用者毎に暗号化コンテンツ開示の可否判断をすることができる。

ここで、前記記録媒体は、それぞれ異なる暗号鍵で暗号化された複数の暗号化コンテンツとそれぞれの暗号化コンテンツを一意に識別するコンテンツ識別子とを対応付けて格納しており、前記開示情報記憶手段は、複数の暗号化コンテンツについて、暗号化コンテンツ毎に前記開示情報を記憶しており、前記開示判断手段は、前記利用者識別子と利用を所望する暗号化コンテンツを識別するコンテンツ識別子とを含む要求を受け付けると、前記開示情報を用いて、前記利用者識別子により識別される利用者に対する前記コンテンツ識別子により識別される暗号化コンテンツの開示の可否を判断するように構成してもよい。

## 【 0 1 0 6 】

この構成によると、管理装置が利用者毎に、複数の暗号化コンテンツのそれぞれについて開示の可否判断をすることができる。

ここで、前記開示情報は、暗号化コンテンツの開示が許可されている期間を示す開示期間、機密を示す機密区分、内容を示す分野の内の少なくとも一つを含むコンテンツ開示情報と、利用者の利用可能期間、利用可能機密区分、利用可能分野の内の少なくとも一つを含む利用者情報とを含み、前記開示判断手段は、前記

コンテンツ情報と前記利用者情報とを参照することにより、前記利用者に対する前記暗号化コンテンツの開示の可否を判断するように構成してもよい。

【0107】

この構成によると、管理装置が利用者毎に、複数個の暗号化コンテンツのそれぞれについて、開示期間、機密区分、分野に応じて、開示の可否判断をすることができる。

ここで、前記管理装置は、更に、前記開示情報を更新する為に用いる更新情報の入力を受け付ける更新受付手段と、受け付けた更新情報に応じて、前記開示情報を更新する更新手段とを備えるように構成してもよい。

【0108】

この構成によると、利用者に配布された暗号化コンテンツを回収して復号鍵を変更することなく、管理装置が状況に応じて開示情報を変更すれば直ちにコンテンツの開示をコントロールすることができる。

ここで、前記管理装置は、更に、前記再生装置からの要求を受け付けると、前記記録媒体及び前記再生装置を有する利用者を一意に識別する利用者識別子と前記暗号化コンテンツを一意に識別するコンテンツ識別子とを含む履歴情報を生成する履歴情報生成手段と、生成した履歴情報を蓄積して記憶する履歴情報記憶手段とを備えるように構成してもよい。

【0109】

この構成によると、管理装置は、利用者が復号鍵を要求した履歴を管理することができる。

また、本発明は、可搬型の記録媒体に格納された暗号化コンテンツを、管理装置から取得した復号鍵を用いて再生する再生装置であって、前記管理装置は、前記暗号化コンテンツの復号鍵を保持しており、前記記録媒体は、暗号鍵により暗号化された暗号化コンテンツと前記管理装置に対して前記復号鍵を要求するための鍵要求プログラムとを格納しており、前記再生装置は、前記記録媒体から、前記鍵要求プログラムを読み出して実行し、前記管理装置から前記復号鍵を受信すると、前記記録媒体から前記暗号化コンテンツを読み出して復号し再生することを特徴とする。

## 【 0 1 1 0 】

この構成によると、再生装置は、記録媒体に格納されている鍵要求プログラムを実行することにより、管理装置に対して復号鍵を要求することができるため、再生装置及び記録媒体を有する真正な利用者のみが復号鍵を要求することができる。

また、本発明のコンテンツ管理システムは、更に、当該システムの管理者が有する管理者装置を備え、前記管理者装置は、前記開示情報を更新する為に用いる更新情報の入力を受け付け、受け付けた更新情報を前記管理装置へ送信し、前記管理装置は、前記管理者装置から前記更新情報を受信し、受信した更新情報に応じて、前記開示情報を更新することを特徴とする。

## 【 0 1 1 1 】

この構成によると、管理装置は、管理者装置からの要求に応じて開示情報を更新するので、当該システムの管理者は状況に応じて開示情報を更新する指示を管理装置へ送信することにより、コンテンツの開示をきめ細かく管理することができる。さらに、変更すると直ちに変更後の情報によるコンテンツの開示の制御が可能である。

## 【 0 1 1 2 】

また、本発明のコンテンツ管理システムは、更に、当該システムの管理者が有する管理者装置を備え、前記管理装置は、前記再生装置からの要求を受け付けると、前記再生装置を有する利用者を一意に識別する利用者識別子と前記暗号化コンテンツを一意に識別するコンテンツ識別子とを含む履歴情報を生成し、生成した履歴情報を蓄積して記憶し、前記管理者装置は、前記管理装置に対して前記履歴情報の送信を要求する履歴要求の入力を受け付け、受け付けた履歴要求を前記管理装置へ送信し、前記管理装置は、前記管理者装置から前記履歴要求を受信し、記憶している前記履歴情報を読み出して前記管理者装置へ送信することを特徴とする。

## 【 0 1 1 3 】

この構成によると、利用者が復号鍵を要求した履歴を管理装置が管理し、当該システムの管理者は管理装置から履歴を取得することができるので、管理者は誰

がどのコンテンツを利用したのかを把握することができる。

【図面の簡単な説明】

【図 1】 コンテンツ管理システム 1 の構成を示す図である。

【図 2】 コンテンツ管理サーバ 1 0 の構成を示すブロック図である。

【図 3】 ユーザ認証テーブル 1 1 0 のデータ構造を示す図である。

【図 4】 ユーザテーブル 1 2 0 のデータ構造を示す図である。

【図 5】 コンテンツテーブル 1 3 0 のデータ構造を示す図である。

【図 6】 復号鍵テーブル 1 4 0 のデータ構造を示す図である。

【図 7】 履歴テーブル 1 5 0 のデータ構造を示す図である。

【図 8】 記録媒体 2 0 に格納されているデータを示す図である。

【図 9】 鍵要求プログラムの動作を示すフローチャートである。

【図 1 0】 コンテンツインデックス出力プログラムの動作を示すフローチャートである。

【図 1 1】 ユーザ用クライアント 3 0 の構成を示すブロック図である。

【図 1 2】 ユーザ認証画面 3 1 0 を示す図である。

【図 1 3】 コンテンツインデックス画面 3 2 0 を示す図である。

【図 1 4】 コンテンツ検索画面 4 1 0 を示す図である。

【図 1 5】 検索結果画面 5 1 0 を示す図である。

【図 1 6】 復号確認画面 6 1 0 を示す図である。

【図 1 7】 復号結果画面 7 1 0 を示す図である。

【図 1 8】 コンテンツ管理システム 1 全体の動作を示すフローチャートである。

【図 1 9】 コンテンツ管理システム 1 におけるコンテンツ開示処理の動作を示すフローチャートである。

【図 2 0】 ユーザ用クライアント 3 0 の制御部 3 0 4 における復号鍵要求処理の動作を示すフローチャートである。

【図 2 1】 コンテンツ管理サーバ 1 0 における復号鍵送信判断処理の動作を示すフローチャートである。

【図 2 2】 コンテンツ管理システム 1 における提供者への履歴情報提供処理の

動作を示すフローチャートである。

【図 2 3】コンテンツ管理システム 1 におけるデータ更新処理の動作を示すフローチャートである。

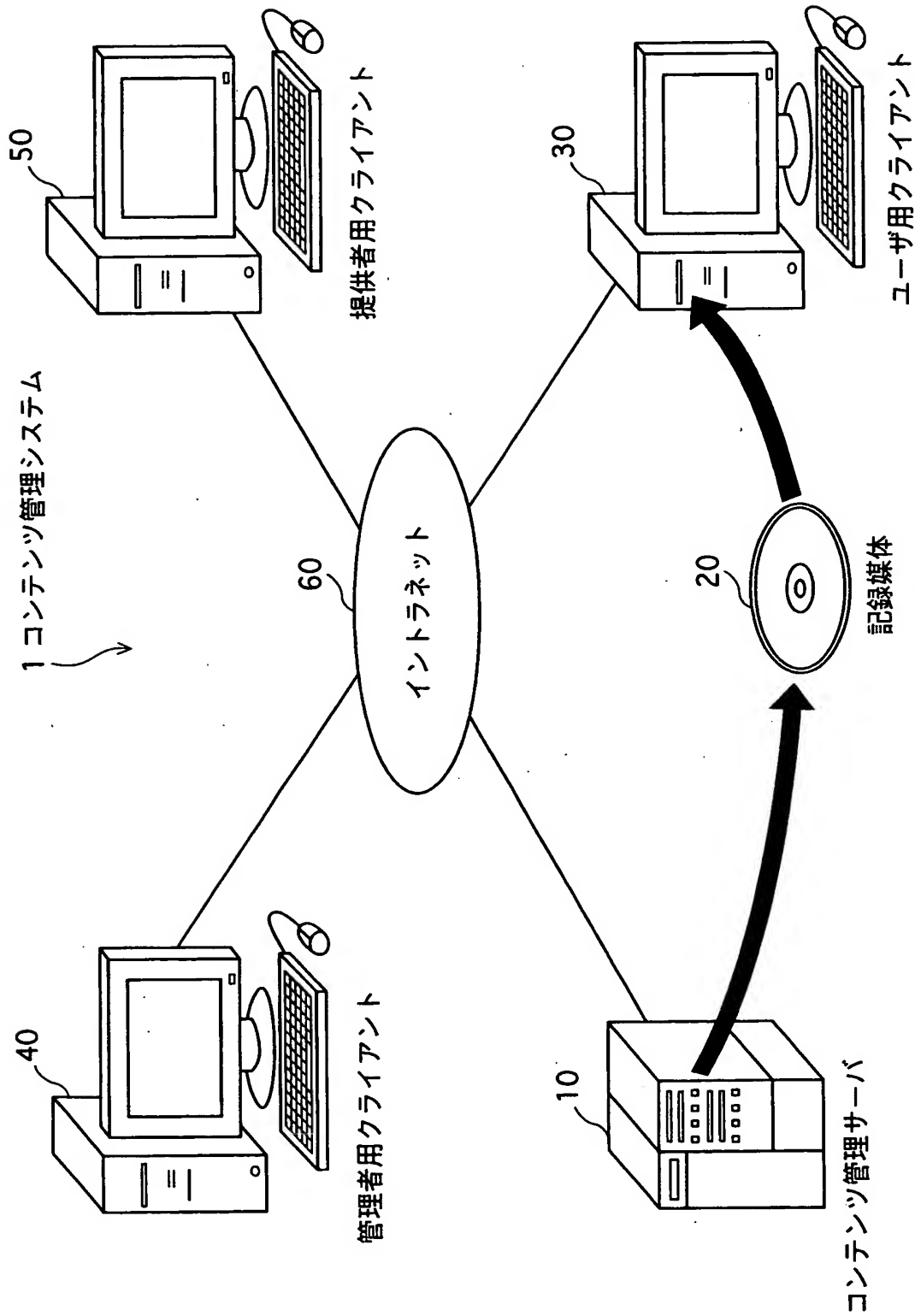
【符号の説明】

- 1     コンテンツ管理システム
- 1 0    コンテンツ管理サーバ
- 2 0    記録媒体
- 3 0    ユーザ用クライアント
- 4 0    管理者用クライアント
- 5 0    提供者用クライアント
- 6 0    イントラネット
- 1 0 1   ゲートウェイ
- 1 0 2   データベース部
- 1 0 3   ユーザ認証部
- 1 0 4   履歴管理部
- 1 0 5   データベース管理部
- 1 0 6   コンテンツ記憶部
- 1 0 7   プログラム記憶部
- 1 0 8   暗号化部
- 1 0 9   入出力部
- 3 0 1   送受信部
- 3 0 2   入力部
- 3 0 3   表示部
- 3 0 4   制御部
- 3 0 4 a   読出部
- 3 0 4 b   解読部
- 3 0 4 c   実行部
- 3 0 5   復号部
- 3 0 6   入出力部

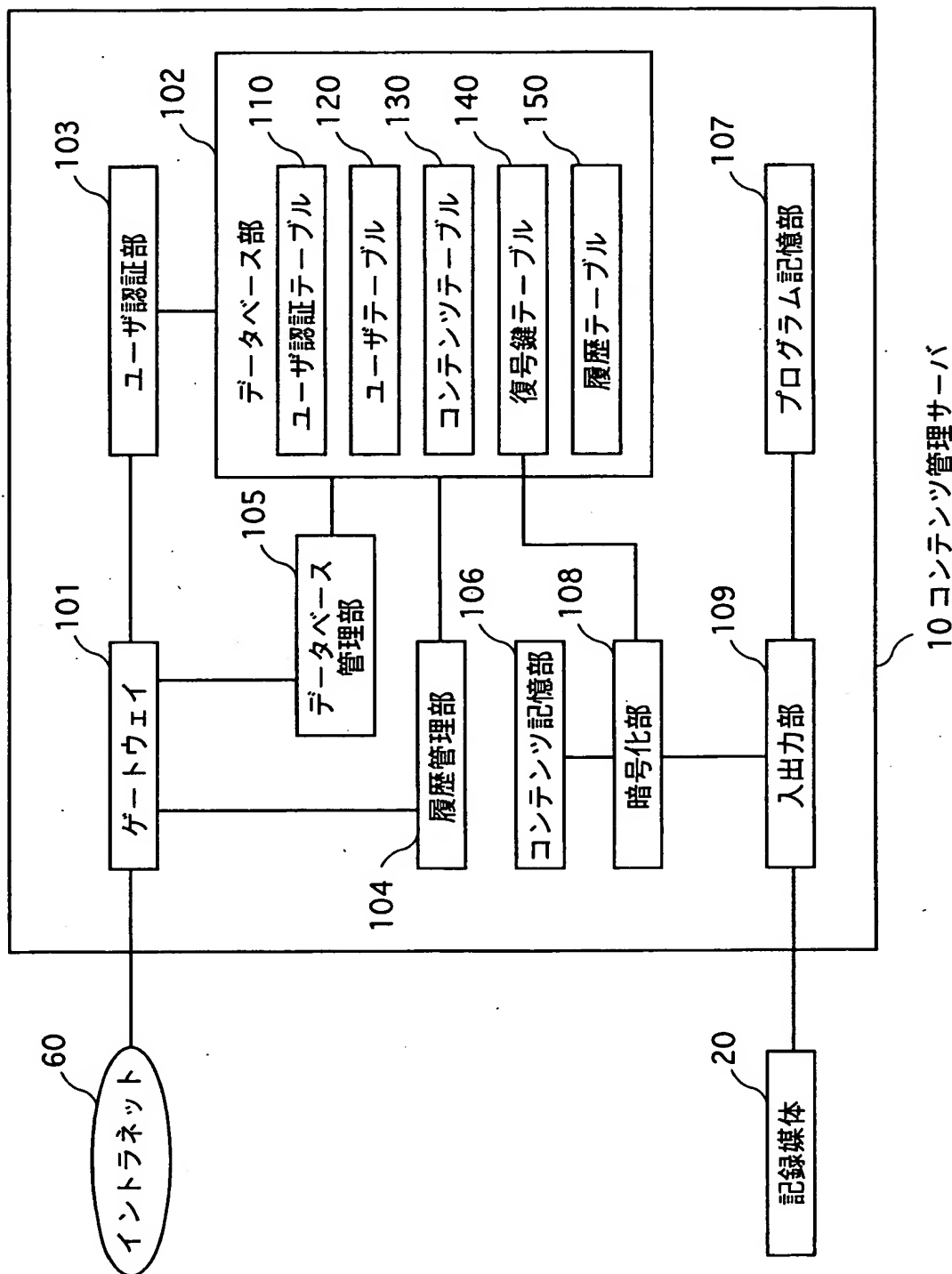
3 0 7 プログラム記憶部

【書類名】 図面

【図 1】



【図 2】





【図 3】

| 1101 ユーザID | 1102 パスワード | 1103 登録ユーザ | 1104 登録日 | 1105 更新ユーザ | 1106 更新日 |
|------------|------------|------------|----------|------------|----------|
| ...        | ...        | ...        | ...      | ...        | ...      |
| ...        | ...        | ...        | ...      | ...        | ...      |
| ...        | ...        | ...        | ...      | ...        | ...      |

110 ユーザ認証テーブル

【図 4】

| 1201  |                | 1202           |            | 1203          |              | 1204      |     | 1205      |     | 1206 |  | 1207 |  | 1208 |  | 1209 |  | 1210 |  |
|-------|----------------|----------------|------------|---------------|--------------|-----------|-----|-----------|-----|------|--|------|--|------|--|------|--|------|--|
| ユーザID | 利用可能<br>期間(開始) | 利用可能<br>期間(終了) | 利用可能<br>件数 | 利用可能<br>分野コード | 利用可能<br>公開区分 | 登録<br>ユーザ | 登録日 | 更新<br>ユーザ | 更新日 |      |  |      |  |      |  |      |  |      |  |
| ⋮     | ⋮              | ⋮              | ⋮          | ⋮             | ⋮            | ⋮         | ⋮   | ⋮         | ⋮   |      |  |      |  |      |  |      |  |      |  |
| ⋮     | ⋮              | ⋮              | ⋮          | ⋮             | ⋮            | ⋮         | ⋮   | ⋮         | ⋮   |      |  |      |  |      |  |      |  |      |  |
| ⋮     | ⋮              | ⋮              | ⋮          | ⋮             | ⋮            | ⋮         | ⋮   | ⋮         | ⋮   |      |  |      |  |      |  |      |  |      |  |

120 ユーザーテーブル

【図 5】

| コンテンツ<br>ID | 公開期間<br>(開始) | 公開期間<br>(終了) | 分野<br>コード | 公開区分 | 登録<br>ユーザ | 登録日 | 更新<br>ユーザ | 更新日 | 提供者<br>ID |
|-------------|--------------|--------------|-----------|------|-----------|-----|-----------|-----|-----------|
| ...         | ...          | ...          | ...       | ...  | ...       | ... | ...       | ... | ...       |
| ...         | ...          | ...          | ...       | ...  | ...       | ... | ...       | ... | ...       |
| ...         | ...          | ...          | ...       | ...  | ...       | ... | ...       | ... | ...       |

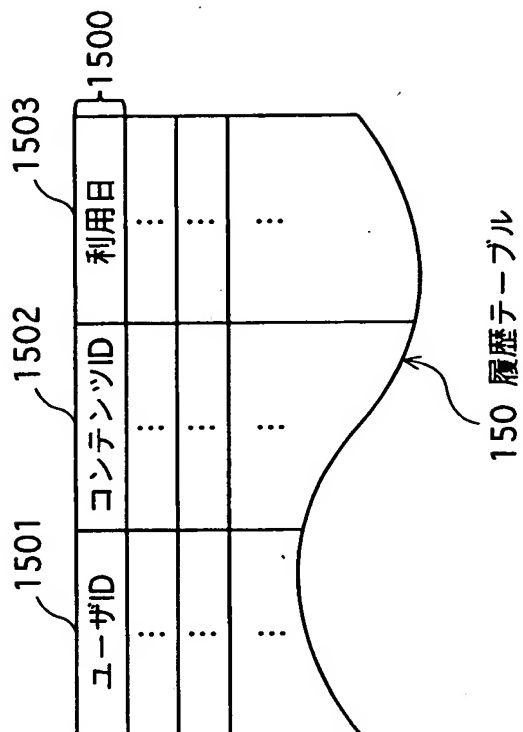
130 コンテンツテーブル

【図 6】

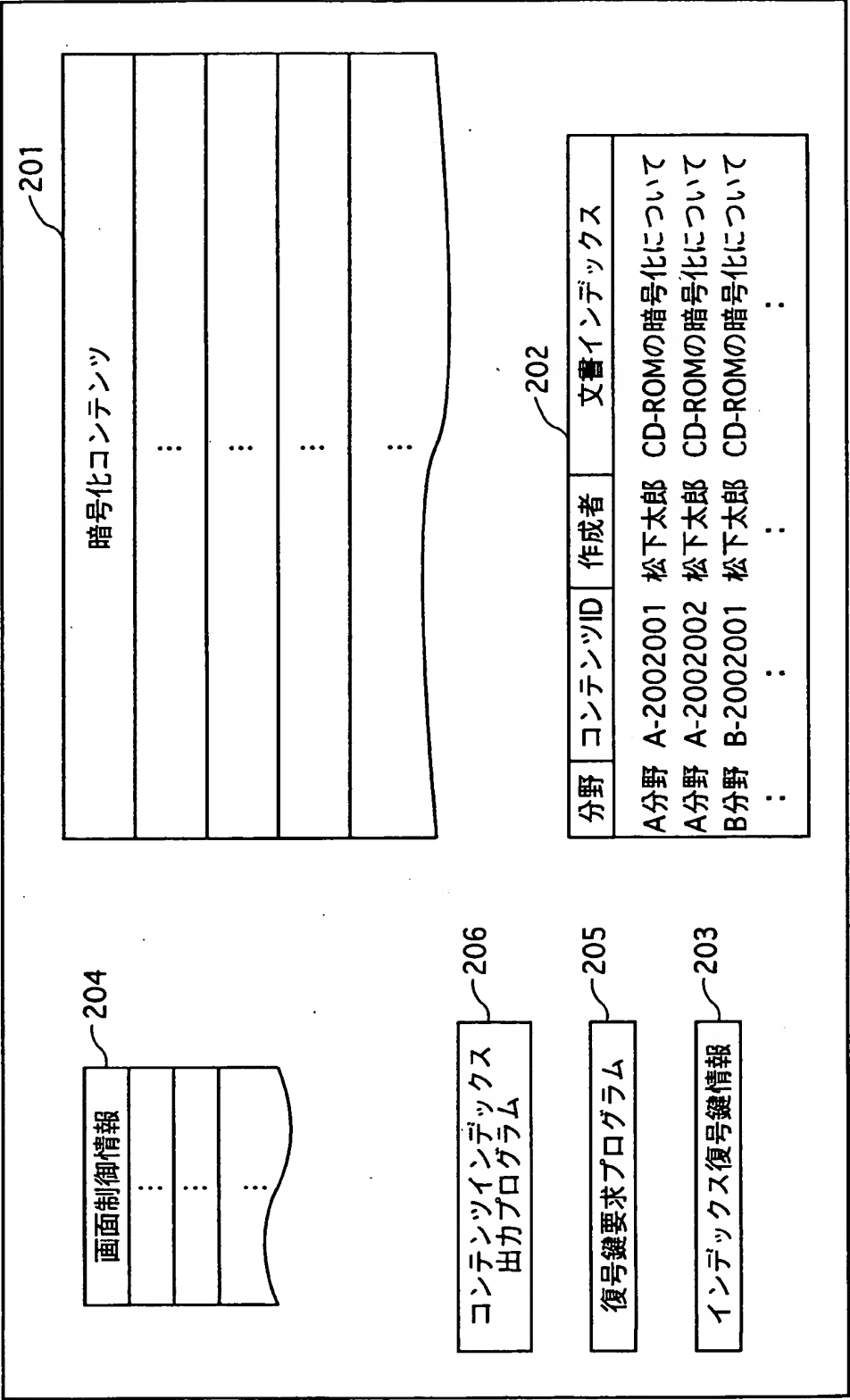
| 1401    |  | 1402 |  | 1403  |  | 1404 |  | 1405  |  | 1406 |
|---------|--|------|--|-------|--|------|--|-------|--|------|
| コンテンツID |  | 復号鍵  |  | 登録ユーザ |  | 登録日  |  | 更新ユーザ |  | 更新日  |
| ⋮       |  | ⋮    |  | ⋮     |  | ⋮    |  | ⋮     |  | ⋮    |
| ⋮       |  | ⋮    |  | ⋮     |  | ⋮    |  | ⋮     |  | ⋮    |
| ⋮       |  | ⋮    |  | ⋮     |  | ⋮    |  | ⋮     |  | ⋮    |

140 復号鍵テーブル

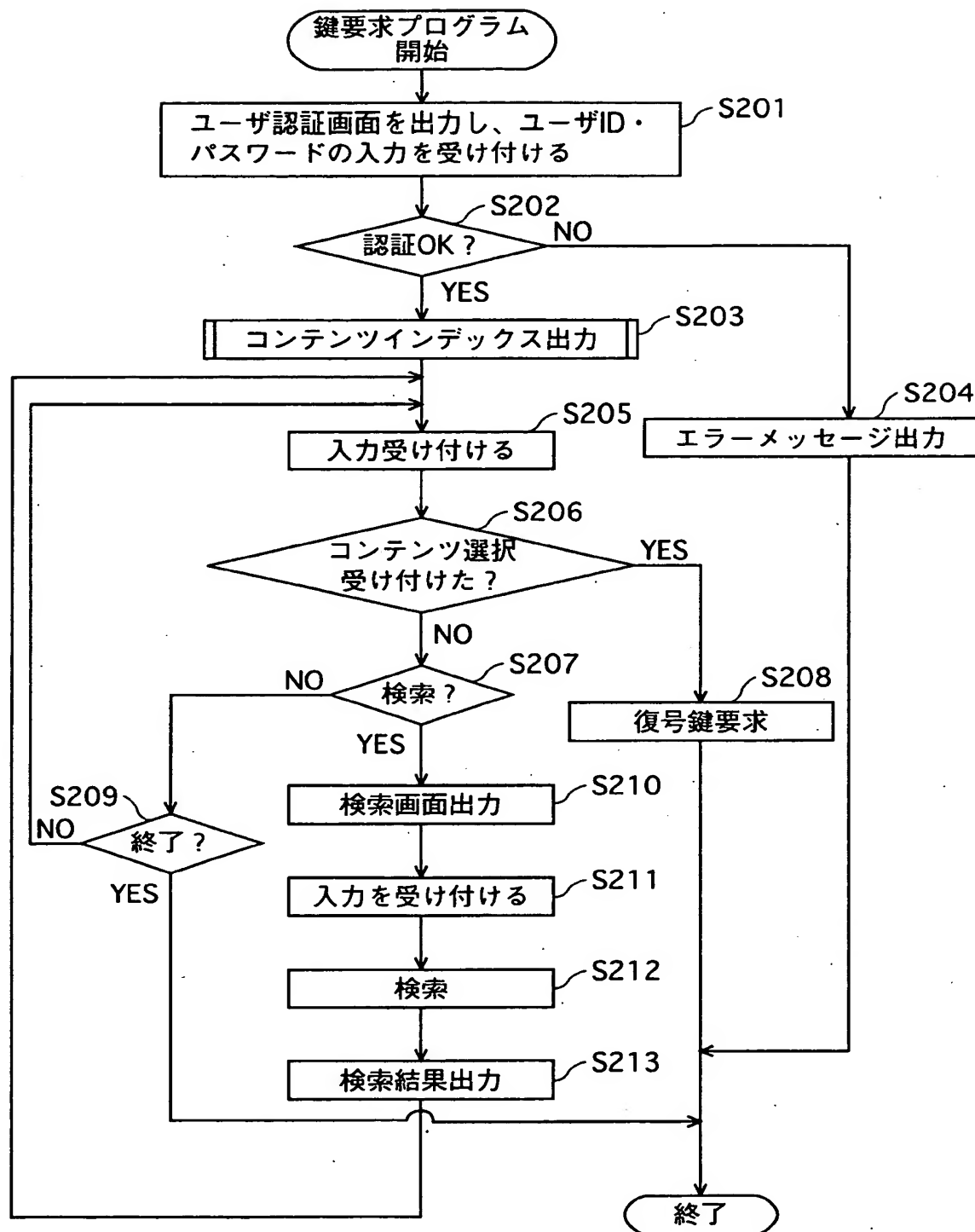
【図 7】



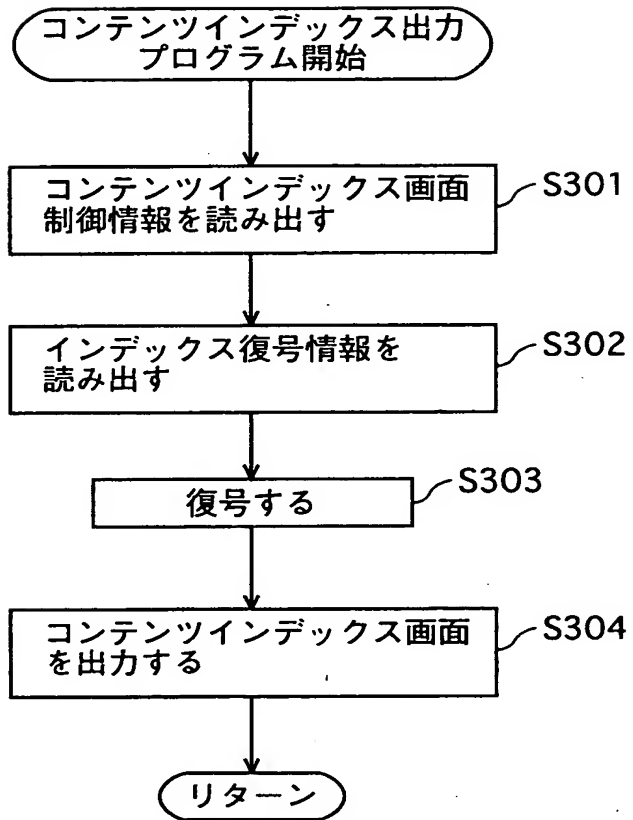
【図 8】



【図9】

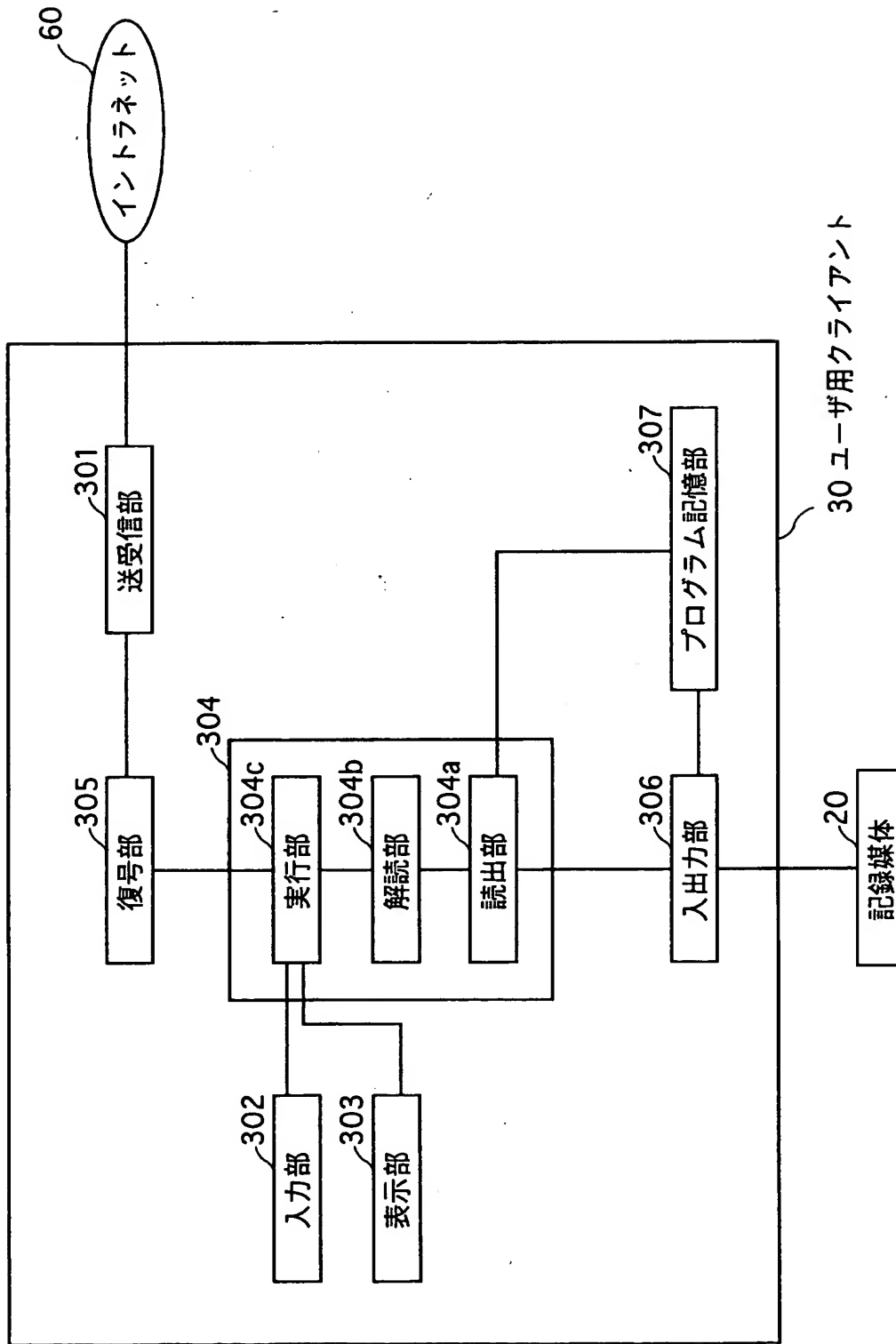


【図 1 0】





【図 11】



【図 1 2】

ユーザID:

パスワード:

OK      キャンセル

【図 1 3】

| 分野  | コンテンツID   | 作成者  | 文書インデックス       |
|-----|-----------|------|----------------|
| A分野 | A-2002001 | 松下太郎 | CD-ROMの暗号化について |
| A分野 | A-2002002 | 松下太郎 | CD-ROMの暗号化について |
| B分野 | B-2002001 | 松下太郎 | CD-ROMの暗号化について |
| :   | :         | :    | :              |

復号する      終了      検索

【図 1 4】

410

コンテンツID: 

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|  |  |  |  |  |

 411

キーワード: 

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|  |  |  |  |  |

 412

作成者: 

|  |
|--|
|  |
|--|

 413

分野: 

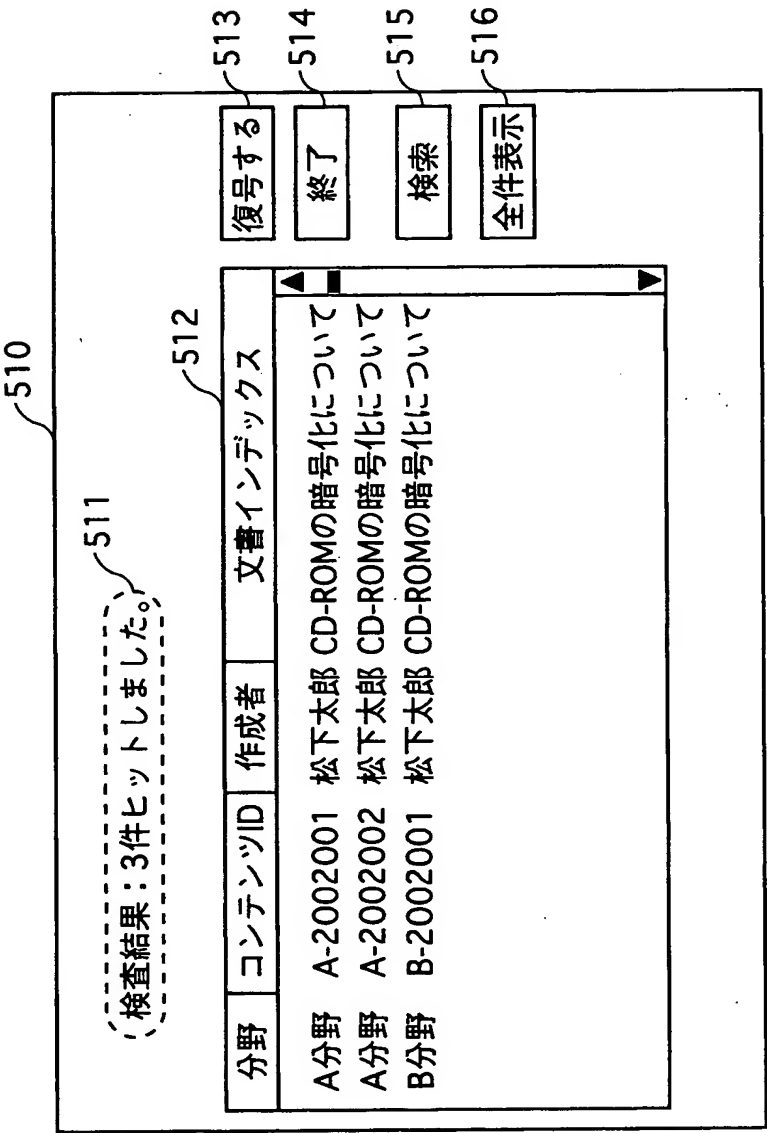
|  |
|--|
|  |
|--|

 414

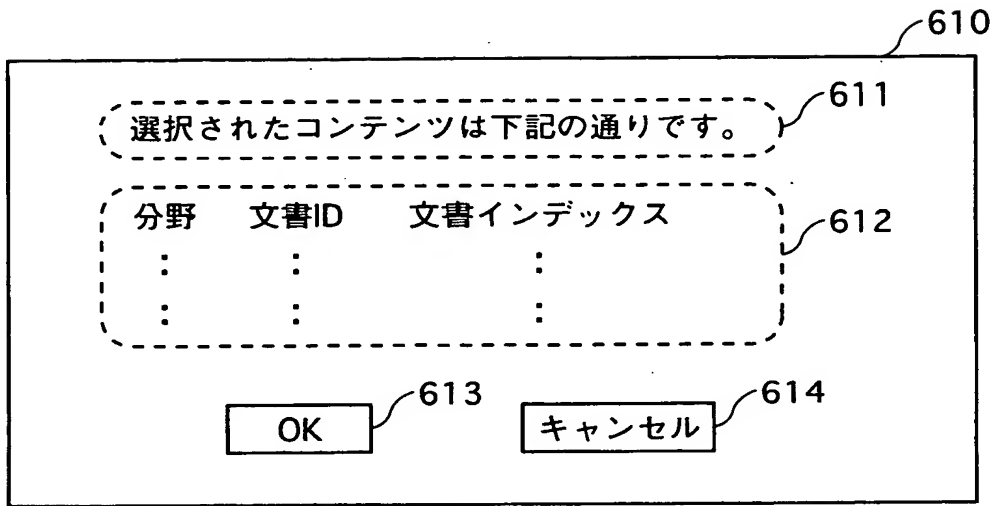
各項目間での検索方法の選択: ☒ AND検索 ☐ OR 415

検索 416      クリア 417      キャンセル 418

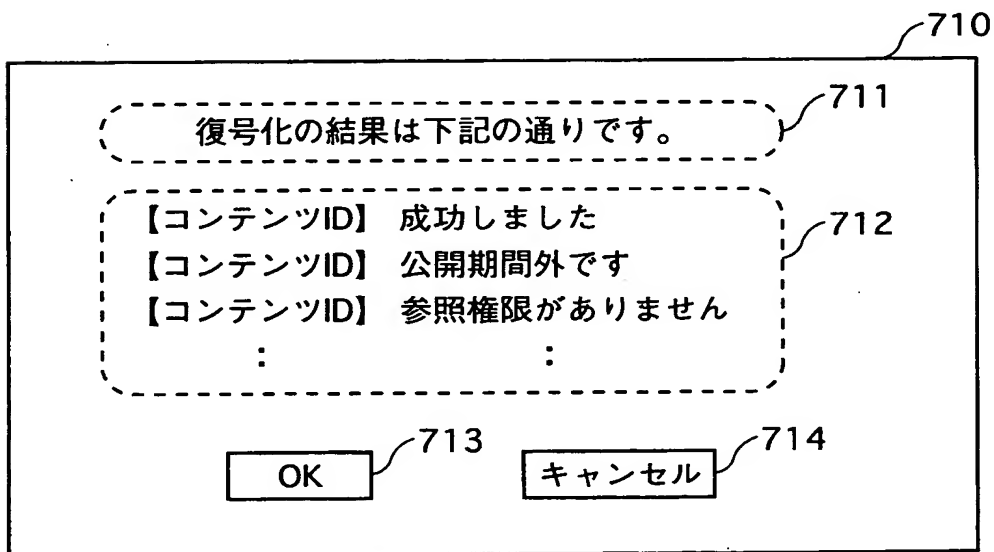
【図 1 5】



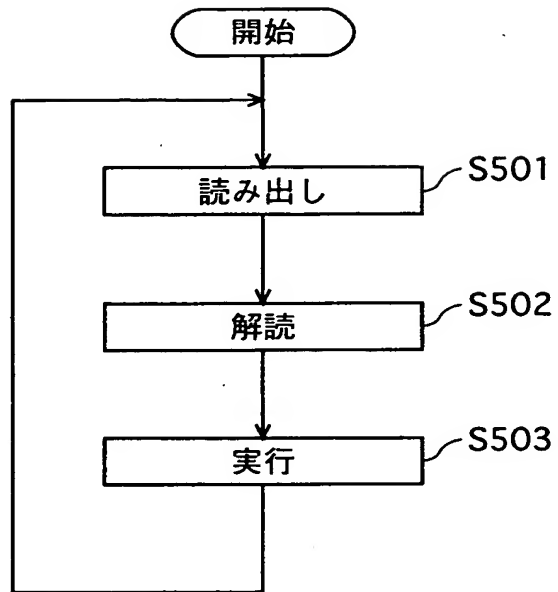
【図16】



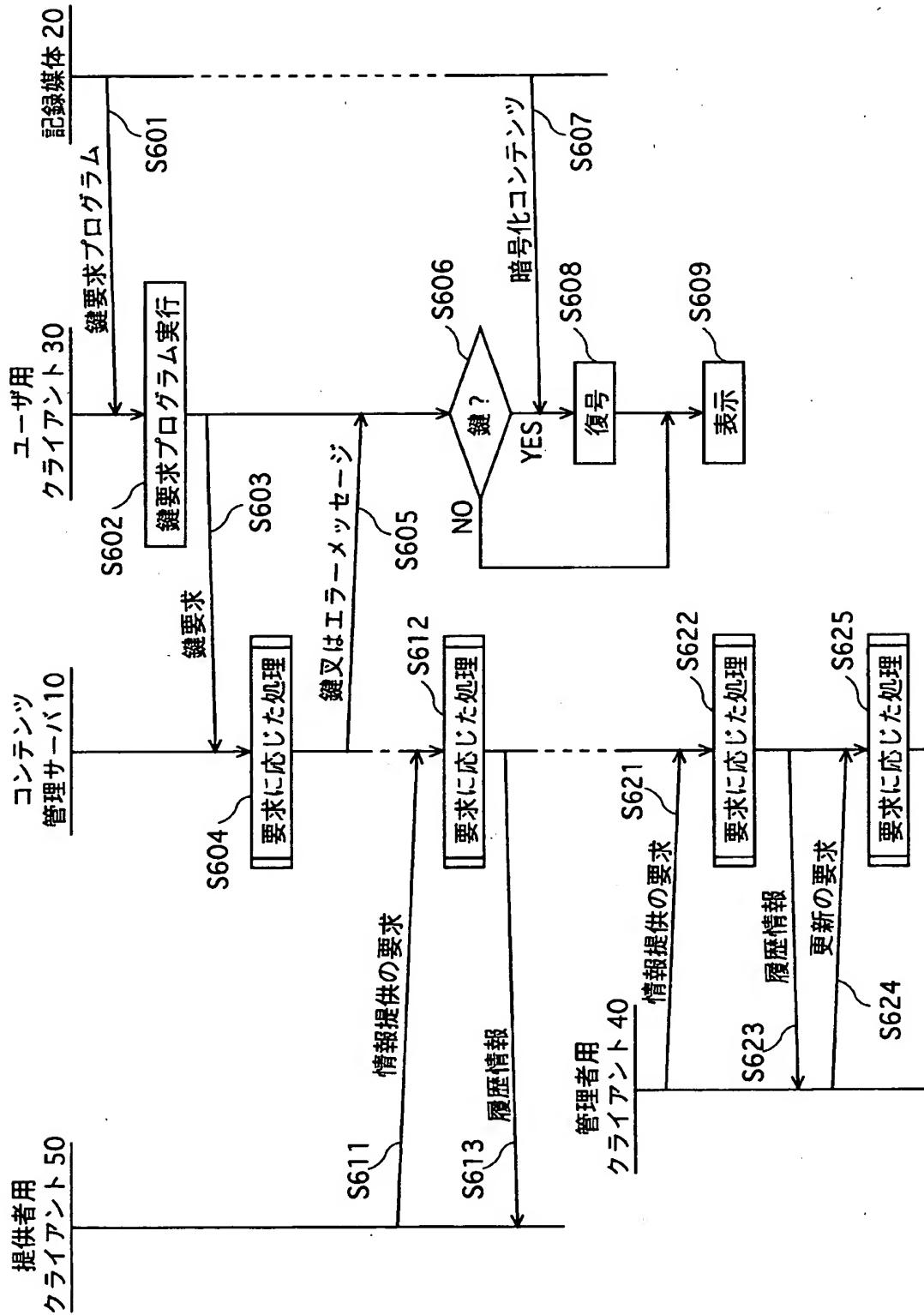
【図17】



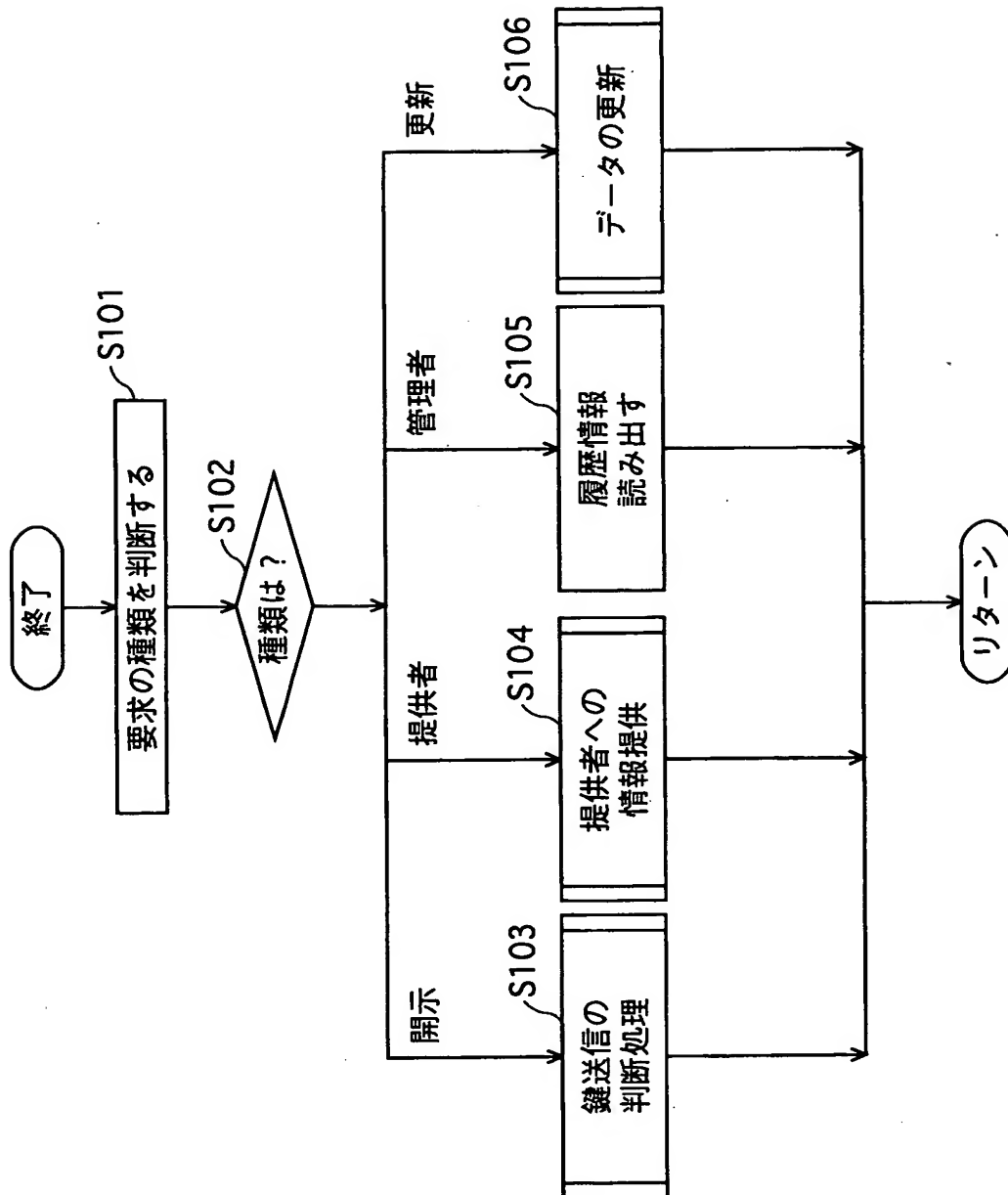
【図 1 8】



【図 19】

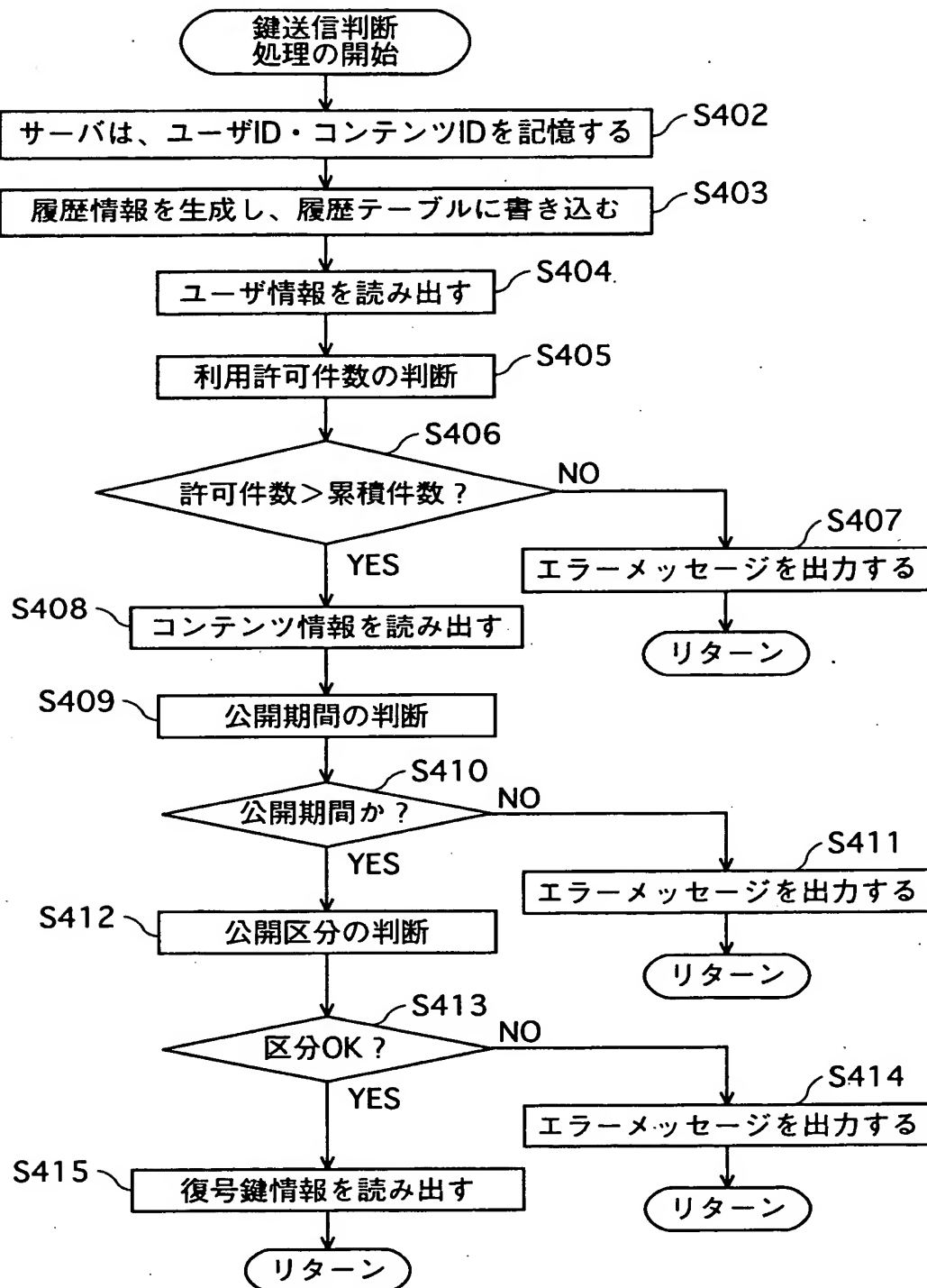


【図20】



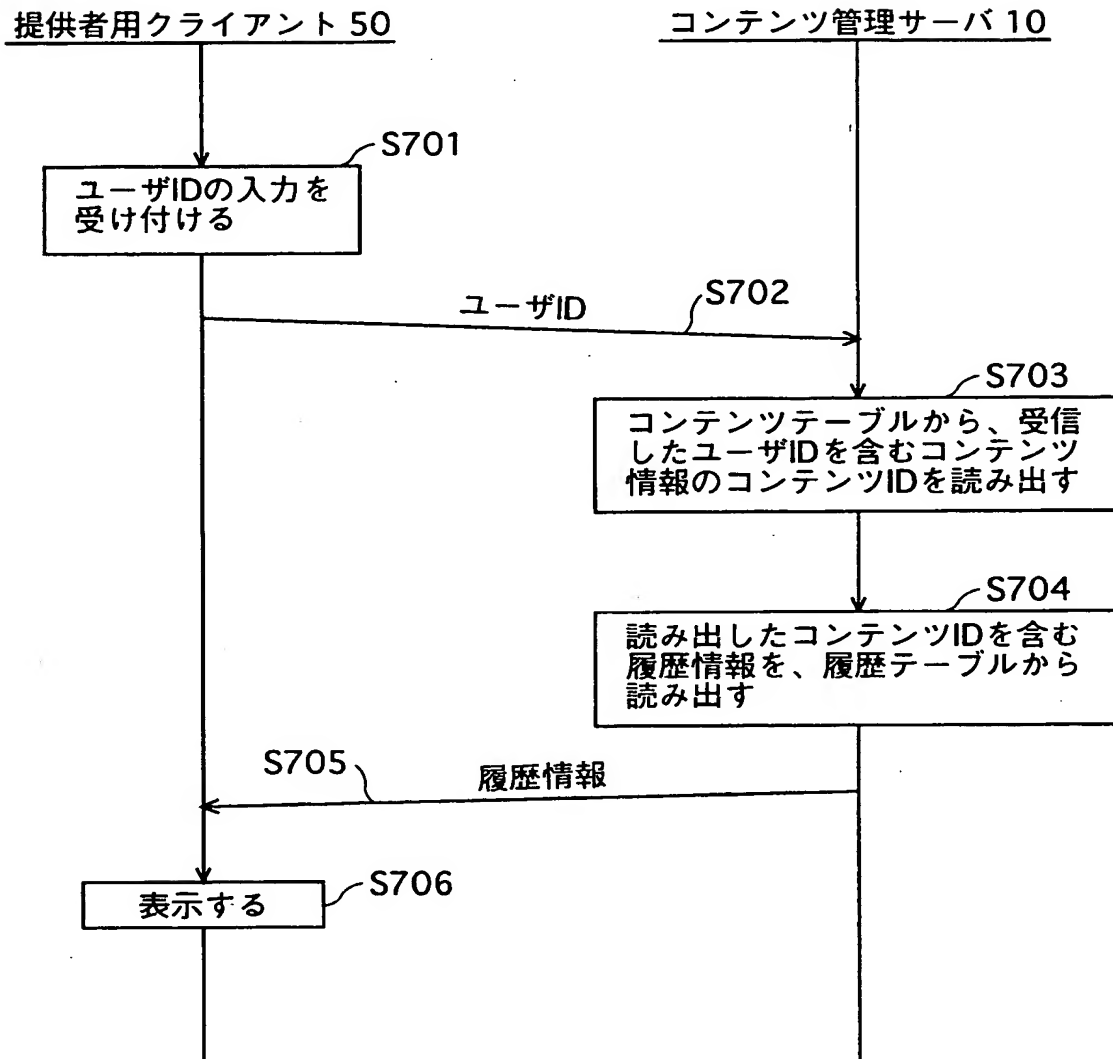


【図 21】



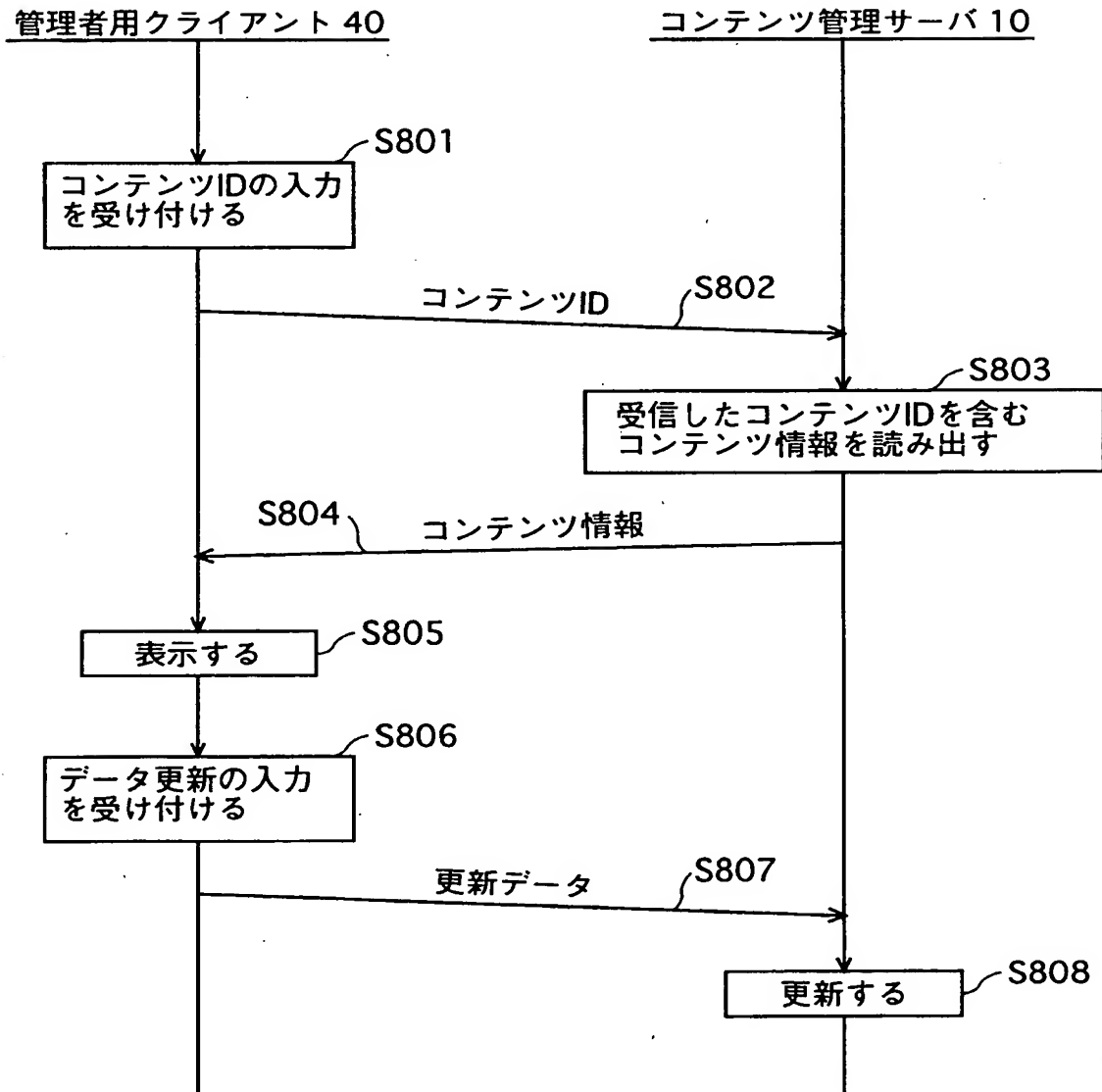
【図 22】

提供者への履歴情報提供の処理



【図 2 3】

データ更新の処理



【書類名】 要約書

【要約】

【課題】 記録媒体に格納されて利用者に配布されたコンテンツの安全性を確保しつつコンテンツの開示に係る権利情報を一元的に管理するコンテンツ管理システムを提供することを目的とする。

【解決手段】 記録媒体 2 0 に格納されて利用者に配布された暗号化コンテンツについて、コンテンツに係る情報と利用者に係る情報とをコンテンツ管理サーバ 1 0 が管理することにより公開期間、公開区分等に応じてコンテンツの開示を制御する。

また、管理者の要求を受けてコンテンツ管理サーバ 1 0 が、コンテンツに係る情報、利用者に係る情報等に含まれる各項目を変更することが可能であり、変更すると直ちに変更後の情報によるコンテンツの開示の制御が可能である。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日  
[変更理由] 新規登録  
住 所 大阪府門真市大字門真1006番地  
氏 名 松下電器産業株式会社